Managing Routers and BNX Platforms

Router Software Version 10.0
Site Manager Software Version 4.0

Software Version BNX 6.0
Site Manager Software Version BNX 6.0

Part No. 112931 Rev. A
January 1996

Bay Networks

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Copyright © 1988–1996 Bay Networks, Inc.

All rights reserved. Printed in the USA. January 1996.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Bay Networks, Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notice for All Other Executive Agencies

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Trademarks of Bay Networks, Inc.

ACE, AFN, BCN, BLN, BN, CN, FRE, LN, Optivity, SynOptics, SynOptics Communications, Wellfleet and the Wellfleet logo are registered trademarks and AN, ANH, ASN, BaySIS, BayStack, BCNX, BLNX, BNX, EZ Internetwork, EZ LAN, FN, PathMan, PhonePlus, PPX, Quick2Config, RouterMan, SPEX, Bay Networks, Bay Networks Press, the Bay Networks logo and the SynOptics logo are trademarks of Bay Networks, Inc.

Third-Party Trademarks

All other trademarks and registered trademarks are the property of their respective owners.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Bay Networks, Inc. reserves the right to make changes to the products described in this document without notice.

Bay Networks, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product are Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Bay Networks Software License

Note: *This is Bay Networks basic license document. In the absence of a software license agreement specifying varying terms, this license — or the license included with the particular product — shall govern licensee's use of Bay Networks software.*

This Software License shall govern the licensing of all software provided to licensee by Bay Networks ("Software"). Bay Networks will provide licensee with Software in machine-readable form and related documentation ("Documentation"). The Software provided under this license is proprietary to Bay Networks and to third parties from whom Bay Networks has acquired license rights. Bay Networks will not grant any Software license whatsoever, either explicitly or implicitly, except by acceptance of an order for either Software or for a Bay Networks product ("Equipment") that is packaged with Software. Each such license is subject to the following restrictions:

1. Upon delivery of the Software, Bay Networks grants to licensee a personal, nontransferable, nonexclusive license to use the Software with the Equipment with which or for which it was originally acquired, including use at any of licensee's facilities to which the Equipment may be transferred, for the useful life of the Equipment unless earlier terminated by default or cancellation. Use of the Software shall be limited to such Equipment and to such facility. Software which is licensed for use on hardware not offered by Bay Networks is not subject to restricted use on any Equipment, however, unless otherwise specified on the Documentation, each licensed copy of such Software may only be installed on one hardware item at any time.
2. Licensee may use the Software with backup Equipment only if the Equipment with which or for which it was acquired is inoperative.
3. Licensee may make a single copy of the Software (but not firmware) for safekeeping (archives) or backup purposes.
4. Licensee may modify Software (but not firmware), or combine it with other software, subject to the provision that those portions of the resulting software which incorporate Software are subject to the restrictions of this license. Licensee shall not make the resulting software available for use by any third party.
5. Neither title nor ownership to Software passes to licensee.
6. Licensee shall not provide, or otherwise make available, any Software, in whole or in part, in any form, to any third party. Third parties do not include consultants, subcontractors, or agents of licensee who have licensee's permission to use the Software at licensee's facility, and who have agreed in writing to use the Software only in accordance with the restrictions of this license.
7. Third-party owners from whom Bay Networks has acquired license rights to software that is incorporated into Bay Networks products shall have the right to enforce the provisions of this license against licensee.
8. Licensee shall not remove or obscure any copyright, patent, trademark, trade secret, or similar intellectual property or restricted rights notice within or affixed to any Software and shall reproduce and affix such notice on any backup copy of Software or copies of software resulting from modification or combination performed by licensee as permitted by this license.

Bay Networks Software License *(continued)*

9. Licensee shall not reverse assemble, reverse compile, or in any way reverse engineer the Software. [Note: For licensees in the European Community, the Software Directive dated 14 May 1991 (as may be amended from time to time) shall apply for interoperability purposes. Licensee must notify Bay Networks in writing of any such intended examination of the Software and Bay Networks may provide review and assistance.]
10. Notwithstanding any foregoing terms to the contrary, if licensee licenses the Bay Networks product "Site Manager," licensee may duplicate and install the Site Manager product as specified in the Documentation. This right is granted solely as necessary for use of Site Manager on hardware installed with licensee's network.
11. This license will automatically terminate upon improper handling of Software, such as by disclosure, or Bay Networks may terminate this license by written notice to licensee if licensee fails to comply with any of the material provisions of this license and fails to cure such failure within thirty (30) days after the receipt of written notice from Bay Networks. Upon termination of this license, licensee shall discontinue all use of the Software and return the Software and Documentation, including all copies, to Bay Networks.
12. Licensee's obligations under this license shall survive expiration or termination of this license.

Contents

About This Guide

Software Suites xix
Audience xx
Before You Begin xx
Bay Networks Customer Support xxi
CompuServe xxi
InfoFACTS xxii
World Wide Web xxii
How to Get Help xxii
Conventions xxiii
Ordering Bay Networks Publications xxiv
Acronyms xxiv

Chapter 1
Overview of Router Management

Configuring the Router 1-1
Monitoring Traps and Events 1-2
Viewing Trap Messages 1-3
Viewing Event Messages 1-6
Monitoring Statistics 1-9
Using the Quick Get Tool 1-10
Using the Screen Builder Tool 1-11
Using the Screen Manager Tool 1-11
Using the Launch Facility Tool 1-11
Using Online Help 1-12
Locating Statistics Files 1-12
Managing Router Files 1-12
Monitoring Changes to Router Configuration Files 1-13
Customizing Router Software Images 1-14

Performing Administrative Functions 1-15
Tracking Network Availability and Response Time 1-16
Keeping a Log 1-17
LOG 1-18

Chapter 2
Using the Trap Monitor

Connecting to a Router 2-1
Configuring the Router's SNMP Agent 2-2
Identifying Site Manager as an SNMP Manager 2-3
Saving a Configuration 2-5
Running Multiple Network Management Applications 2-6
Configuring Traps Sent by a Router 2-8
Specifying Traps by Category 2-8
Specifying Traps by Entity 2-10
Specifying Traps by Event Type 2-12
Enabling an SNMP Agent 2-14
Viewing Trap Messages 2-16
Using the Trap Monitor 2-16
Displaying the Trap History File 2-16
Filtering Trap Messages 2-17
Filtering by Severity 2-18
Filtering by Router IP Address 2-18
Clearing the Trap Monitor Window 2-20
Clearing the Trap History File 2-20
Saving Trap Messages 2-21

Chapter 3
Monitoring Router Events

Connecting to a Router 3-1
Displaying Event Logs 3-2
Displaying the Current Log 3-2
Displaying a Remote Log 3-4
Displaying a Local Log 3-5
Filtering Event Messages 3-6
Filtering by Severity, Slot, and Entity 3-6

Filtering by Router IP Address 3-8
Searching for an Event Message 3-8
Refreshing the Events Manager Window 3-9
Clearing the Events Manager Window 3-9
Saving Event Messages 3-9
Clearing the Current Event Log 3-11

Chapter 4
Monitoring Statistics

Accessing Statistics 4-1
Connecting to a Router 4-2
Viewing the Bay Networks MIB 4-3
Using the MIB Browser 4-5
Getting Instances of Selected Objects 4-7
Defining the Current Screen List 4-13
Adding Statistics Screens 4-13
Removing Statistics Screens 4-15
Displaying Statistics Screens 4-16
Refreshing Active Statistics Screens 4-17
Specifying Circuit Mode Statistics Polling Rate 4-17
Zeroing Circuit Mode Statistics 4-18
Zeroing All Counters in a Screen 4-18
Zeroing All Counters in a Specific Row 4-20
Stopping Statistics Retrieval 4-21
Creating Statistics Filters 4-21
Using Display Filters 4-22
Using Retrieval Filters 4-25
Searching for Statistics Information 4-26
Saving Statistics Information 4-27
Building Custom Statistics Screens 4-28
Designing Statistics Screens 4-28
Displaying Custom Statistics Screens 4-33
Editing Custom Statistics Screens 4-33
Retrieving a Statistics Screen File 4-33
Editing a Statistics Screen File 4-34
Using the MIB II Counters Feature 4-35

For More Information 4-37

Chapter 5
Managing Router Files

Displaying the Contents of a Volume 5-2
Active Volumes 5-3
Available and Contiguous Free Space 5-4
Default Filenames 5-5
Connecting to a Router 5-6
Naming a File 5-7
Copying a File 5-8
Examining the Router Destination Volume 5-8
Verifying Adequate Free Space 5-8
Creating the Copy 5-9
Deleting a File 5-10
Transferring a File 5-11
Setting Up Multiple Routers 5-13
Getting a File 5-16
Putting a File 5-19
Choosing the Routers 5-19
Examining the Router Destination Volume 5-19
Verifying Adequate Free Space on the Destination Volume 5-20
Transferring Files to the Destination Volume 5-21
Backing Up Router Software Files to a Host Computer 5-23
Modifying config Files in Remote Configuration Mode 5-23
Compacting File Space on a Flash Memory Card 5-24
Formatting a Memory Card or Flash SIMM 5-26
Partitioning Media on Bay Networks Routers 5-26
Creating a Partition 5-27
Deleting a Partition 5-30

Chapter 6
Using the Report Generator and Audit Trail Feature

Generating Configuration File Reports 6-1
Generating Reports from Site Manager 6-1
Generating Configuration File Reports from UNIX 6-8

Generating Configuration File Reports from Windows 6-9
For More Information 6-10
Maintaining an Audit Trail Log 6-11
Editing the Audit Trail Configuration File 6-11
Viewing an Audit Trail Log File 6-13

Chapter 7
Performing Administrative Functions

Router Booting Procedures 7-1
FN/LN/CN Router Boot Prerequisite 7-2
Booting a Router 7-2
Using Delayed Boot 7-4
Enabling and Disabling Delayed Boot 7-5
Scheduling a Delayed Boot 7-5
Modifying a Scheduled Delayed Boot 7-9
Deleting a Scheduled Delayed Boot 7-9
Deleting All Scheduled Delayed Boots 7-10
Specifying Values for Delayed Boot Parameters 7-10
Booting a Processor Module 7-13
Clearing the Event Log 7-15
Setting a Router's Date and Time 7-15
Pinging a Remote Device 7-16
IP Ping 7-17
IP Ping Responses 7-19
IPX Ping 7-20
IPX Ping Responses 7-22
OSI Ping 7-22
OSI Ping Responses 7-23
VINES Ping 7-24
VINES Ping Responses 7-26
AppleTalk Ping 7-27
AppleTalk Ping Responses 7-28
APPN Ping 7-29
APPN Ping Responses 7-30
Reallocating Memory Partitions for a Processor Module 7-31
Partitioning Overview 7-32

Repartitioning Global and Local Memory 7-33

Chapter 8
Using the Ping MIB

Configuring IP Ping Requests 8-1
Specifying Values for Ping at Intervals Parameters 8-6
Deleting Ping Requests 8-11
Specifying Source Routes 8-12
Changing or Deleting Source Route Addresses 8-13
Reviewing IP Ping Statistics 8-14
Removing Entries from the Ping MIB 8-14

Appendix A
Responding to SNMP SET Errors

Accessing the SNMP SET Error Log A-2
UNIX Workstations A-3
DOS Workstations A-3

Appendix B
Using the syslog Facility

Configuring the *syslogd* Daemon B-2
Understanding How *syslog* Filters Messages B-3
Configuring the *syslog* Facility B-3
Configuring *syslog* Group Parameters B-4
syslog Group Parameters B-5
Configuring the *syslog* Host List B-7
syslog Host Filter List Parameters B-11
syslog Host List Parameters B-19
Deleting the *syslog* Facility from the Router B-21

Appendix C
Generating Binary Configuration Files

Preparing the ASCII Configuration File C-1
Using Config Generator C-2
Checking for Errors C-2
Checking MIB Attributes C-3
Checking MIB Attribute Values C-3
Identifying Files Created by Config Generator C-4

Index

Figures

Figure 1-1. Bay Networks Trap Monitor Window 1-4
Figure 1-2. Events Manager Window 1-7
Figure 1-3. Statistics Manager Tools Menu 1-9
Figure 1-4. Site Manager Administration Menu Window 1-16
Figure 2-1. Router Connection Options Window 2-2
Figure 2-2. Configuration Manager Window 2-3
Figure 2-3. SNMP Community List Window 2-4
Figure 2-4. SNMP Manager List Window 2-4
Figure 2-5. Add SNMP Manager Window 2-5
Figure 2-6. Trap Port and Trap Types Window 2-7
Figure 2-7. Specifying a Trap Category 2-9
Figure 2-8. Trap Configuration Window 2-11
Figure 2-9. Traps Exceptions Lists Window 2-12
Figure 2-10. Add Trap Window 2-13
Figure 2-11. Traps Exceptions Lists Window 2-14
Figure 2-12. Edit SNMP Global Parameters Window 2-15
Figure 2-13. Values Selection Window 2-15
Figure 2-14. Trap Monitor Window 2-17
Figure 2-15. Selected Trap-Types Window 2-18
Figure 2-16. Address Filters Window 2-19
Figure 2-17. Sample Address Filters Window 2-20
Figure 2-18. Saving Traps to a File 2-21
Figure 3-1. Router Connection Options Window 3-2
Figure 3-2. Events Manager Window 3-3
Figure 3-3. Load Remote Log File Window 3-4
Figure 3-4. Load Local Log Window 3-5
Figure 3-5. Filtering Parameters Window 3-7
Figure 3-6. Find Text Pattern Window 3-8
Figure 3-7. Save Log Window 3-10

Figure 3-8. Confirmation Window 3-11
Figure 4-1. Statistics Manager Window 4-2
Figure 4-2. Router Connection Options Window 4-3
Figure 4-3. Quick Get Facility Window 4-4
Figure 4-4. MIB Tree for System Group 4-5
Figure 4-5. Sample Quick Get Facility Window 4-7
Figure 4-6. All Instances Retrieved (Unfiltered) without Instance IDs 4-9
Figure 4-7. All Instances Retrieved (Unfiltered) with Instance IDs 4-10
Figure 4-8. Specific Instances Retrieved without Instance IDs 4-11
Figure 4-9. Specific Instances Retrieved with Instance IDs 4-12
Figure 4-10. Screen Manager Window 4-14
Figure 4-11. Example of Filename and Screen Description 4-14
Figure 4-12. Statistics Launch Facility Window 4-16
Figure 4-13. Statistics Screen 4-17
Figure 4-14. Polling Rate Window 4-18
Figure 4-15. Zeroing All Counters in a Screen 4-19
Figure 4-16. Zeroing All Counters in a Specific Row 4-20
Figure 4-17. Display Filters Window 4-22
Figure 4-18. Statistics Window Unfiltered 4-23
Figure 4-19. Sample Display Filters Window 4-24
Figure 4-20. Statistics Screen after Filter Implemented 4-24
Figure 4-21. Retrieval Filters Window 4-25
Figure 4-22. Statistics Screen after Implementing a Retrieval Filter 4-26
Figure 4-23. Search Options Window 4-26
Figure 4-24. Screen Builder Facility Window 4-28
Figure 4-25. Screen Builder Column Total Window 4-30
Figure 4-26. Selecting Columns to Total 4-31
Figure 4-27. Statistics Save/Load Screen 4-32
Figure 4-28. MIB II Counters Enable/Disable Window 4-37
Figure 5-1. Router Files Manager Window 5-2
Figure 5-2. Volume Box in Router Files Manager Window 5-4
Figure 5-3. Router Connection Options Window 5-7
Figure 5-4. Copy File Window for Source Filename 5-9
Figure 5-5. Copy File Window for Destination Filename 5-10
Figure 5-6. Deleting Router Files 5-11

Figure 5-7. Selecting the TFTP Option 5-12
Figure 5-8. Multiple Router Setup Window 5-14
Figure 5-9. Adding Routers to the Current Routers List 5-15
Figure 5-10. Multiple Router Setup Window 5-16
Figure 5-11. TFTP Get Files Window 5-17
Figure 5-12. TFTP Rename Files Window 5-18
Figure 5-13. TFTP Put File Selection Window 5-21
Figure 5-14. TFTP Rename Files Window 5-22
Figure 5-15. Create Partition Confirmation Window 5-28
Figure 5-16. Volume Identifiers for Partitioned Media 5-29
Figure 5-17. Delete Partition Confirmation Window 5-30
Figure 6-1. Configuration Report Generator Window 6-2
Figure 6-2. Select Configuration File Window 6-4
Figure 6-3. Save Report File As Window 6-5
Figure 6-4. Use Report Template File Window 6-6
Figure 6-5. Sample Configuration File Report 6-7
Figure 6-6. Default Audit Trail Configuration File 6-11
Figure 6-7. Sample Audit Trail Log File 6-13
Figure 7-1. Boot Router Window 7-3
Figure 7-2. RUI Boot Group List Window 7-5
Figure 7-3. RUI Boot Interface Parameters Window 7-6
Figure 7-4. RUI Boot Parameters Window 7-7
Figure 7-5. Delete RUI Boot Message Window 7-10
Figure 7-6. Reset Slot Window 7-14
Figure 7-7. Selecting a Slot 7-14
Figure 7-8. Router Date and Time Window 7-16
Figure 7-9. Selecting Ping from Router Option 7-17
Figure 7-10. IP Ping Window 7-18
Figure 7-11. Ping Is Alive Window 7-19
Figure 7-12. Ping Does Not Respond Window 7-19
Figure 7-13. IPX Ping Window 7-21
Figure 7-14. OSI Ping Window 7-23
Figure 7-15. VINES Ping Window 7-25
Figure 7-16. AppleTalk Ping Window 7-27
Figure 7-17. APPN Ping Window 7-29

Figure 7-18. Specifying Router Connection Options 7-33
Figure 7-19. Kernel Configuration Window 7-34
Figure 8-1. Router Connection Options Window 8-2
Figure 8-2. File Selection Window 8-3
Figure 8-3. Configuration Manager Window 8-4
Figure 8-4. Ping at Intervals Window 8-5
Figure 8-5. IP Ping Parameters Window 8-5
Figure 8-6. Source Route Entries Window 8-12
Figure 8-7. Source Ping Parameters Window 8-12
Figure A-1. Sample SNMP SET Error Message A-1
Figure A-2. Logged Version of SNMP SET Error Message A-2
Figure B-1. Syslog Group Parameters Window B-4
Figure B-2. Syslog Host List Window B-7
Figure B-3. Syslog Remote Host Configuration Window B-8
Figure B-4. Syslog Host Filter List Window B-8
Figure B-5. Syslog Filter Config Window B-9

Tables

Table 1-1. Comparing Trap Messages and Event Messages 1-3
Table 1-2. Trap Message Details 1-5
Table 1-3. Event Message Details 1-8
Table 1-4. Statistics Manager Tools 1-10
Table 2-1. Restarting Site Manager on a New Port 2-8
Table 2-2. Categories of Traps 2-9
Table 2-3. Entering Values in the Add Trap Window 2-13
Table 4-1. Finding MIB Information 4-6
Table 4-2. MIB II Counters 4-36
Table 5-1. Active Volume Representations 5-3
Table 5-2. Free Space Fields in Router Files Manager Window 5-5
Table 5-3. Default Router Filenames 5-5
Table 6-1. Output Format Options 6-2
Table 6-2. Options for Command Line (UNIX) 6-8
Table 6-3. Options for Command Line (Windows) 6-9
Table 7-1. Delayed Boot Parameter Fields and Acceptable Values 7-8
Table 7-2. Delayed Boot Fields and Values 7-12
Table 8-1. Default Ping MIB Statistics Screens 8-14
Table B-1. syslogd Error Levels B-17

About This Guide

If you are responsible for configuring and managing Bay Networks routers and/or BNX platforms, you need to read this guide for instructions on

- Accessing and viewing trap messages and event messages
- Accessing and viewing statistics
- Managing router files
- Monitoring changes to router configuration files
- Basic system administration
- Tracking network availability and response time

This guide primarily covers how you perform these tasks using the Bay Networks Site Manager application.

Note: *The Site Manager windows shown in this book are from an X Window System UNIX environment. Minor variations in screen appearance may occur from platform to platform.*

Software Suites

Routing and Switching software is available in the following suites:

- The *System Suite* includes IP routing, 802.1 Transparent Bridge, Source Route Bridge, Translation Bridge, SNMP Agent, Bay Networks HDLC, PPP, OSPF, EGP, BGP, and basic DLSw.
- The *LAN Suite* includes DECnet Phase 4, AppleTalk Phase 2, OSI, VINES, IPX, and ATM DXI, in addition to the System Suite.
- The *WAN Suite* includes ATM DXI, Frame Relay, LAPB, and X.25, in addition to the System Suite.
- The *Corporate Suite* includes the System, LAN, and WAN suites in their entirety.

- The *ARE ATM Suite* provides RFC 1483 and 1577 compliance, ATM UNI 3.0 signaling, in addition to the LAN Suite.
- The *ARE VNR Corporate Suite* provides ATM Forum LAN Emulation, in addition to the ARE ATM Suite and Corporate Suite.
- The *BNX Suite* includes IP Routing, SNMP Agent, Bay Networks HDLC, PPP, OSPF, EGP, BGP, File-Based Performance Statistics, Frame Relay switching, and Frame Relay billing, and selected components from the Corporate, ARE ATM, and ARE VNR Corporate suites.

Availability of features and functionality described in this guide depends on the suites you are using.

Audience

This guide is intended for experienced network operators who have a technical understanding of data communications.

You should have a basic understanding of how Site Manager works. You perform some of the management tasks in this guide using commands and utilities that you access directly from your workstation's operating system (such as UNIX or DOS). To use these commands and utilities, you should be familiar with your workstation's operating system and a standard text editor.

Before You Begin

Refer to the following:

- *Quick-Starting Routers and BNX Platforms* for information on how to install Site Manager on your computer
- *Using Site Manager Software* for an introduction to the Bay Networks network management application
- *Configuring Routers* or *Configuring Customer Access and Trunks (BNX Software)* for information on how to use the Configuration Manager tool
- *Configuring SNMP, BOOTP, DHCP, and RARP Services* for more information on SNMP

Bay Networks Customer Support

Bay Networks provides live, telephone technical support to our distributors, resellers, and service-contracted customers from two U.S. and three international support centers. If you have purchased your Bay Networks product from a distributor or authorized reseller, contact the technical support staff of that distributor or reseller for assistance with installation, configuration, troubleshooting, or integration issues.

Customers also have the option of purchasing direct support from Bay Networks through a variety of service programs. The programs include priority access telephone support, on-site engineering assistance, software subscription, hardware replacement, and other programs designed to protect your investment.

To purchase any of these support programs, including PhonePlus™ for 24-hour, telephone technical support, call 1-800-2LANWAN. Outside the U.S. and Canada, call (408) 764-1000. You can also receive information on support programs from your local Bay Networks field sales office, or purchase Bay Networks support directly from your reseller. Bay Networks provides several methods of receiving support and information on a nonpriority basis through the following automated systems.

CompuServe

Bay Networks maintains an active forum on CompuServe. All you need to join us online is a computer, a modem, and a CompuServe account. We also recommend using the CompuServe Information Manager software, available from CompuServe.

The Bay Networks forum contains libraries of technical and product documents designed to help you manage and troubleshoot your Bay Networks products. Software agents and patches are available, and the message boards are monitored by technical staff and can be a source for problem solving and shared experiences.

Customers and resellers who have Bay Networks service contracts can visit the special libraries to acquire advanced levels of support documentation and software.

To open an account and receive a local dial-up number, call CompuServe at 1-800-524-3388 and ask for Representative No. 591.

- In the United Kingdom, call Freephone 0800-289378.

- In Germany, call 0130-37-32.
- In Europe (except for the United Kingdom and Germany), call (44) 272-760681.
- Outside the U.S., Canada, and Europe, call (614) 529-1349 and ask for Representative No. 591, or consult your listings for an office near you.

Once you are online, you can reach our forum by typing the command **GO BAYNETWORKS** at any ! prompt.

InfoFACTS

InfoFACTS is the Bay Networks free, 24-hour, fax-on-demand service. This automated system contains libraries of technical and product documents designed to help you manage and troubleshoot your Bay Networks products. The system can return a fax copy to the caller or to a third party within minutes of being accessed.

World Wide Web

The World Wide Web (WWW) is a global information system for file distribution and online document viewing via the Internet. You need a direct connection to the Internet and a Web Browser (such as Mosaic or Netscape).

Bay Networks maintains a WWW Home Page that you can access at http://www.baynetworks.com. One of the menu items on the Home Page is the Customer Support Web Server, which offers technical documents, software agents, and an E-mail capability for communicating with our technical support engineers.

How to Get Help

For additional information or advice, contact the Bay Networks Technical Response Center in your area:

United States	1-800-2LAN-WAN
Valbonne, France	(33) 92-966-968
Sydney, Australia	(61) 2-903-5800
Tokyo, Japan	(81) 3-328-005

Conventions

This section describes the conventions used in this guide.

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: if command syntax is **ping** *<ip_address>*, you enter **ping 192.32.10.12**
arrow character (➔)	Separates menu and option names in instructions. Example: Protocols➔AppleTalk identifies the AppleTalk option in the Protocols menu.
bold text	Indicates text that you need to enter and command names in text. Example: Use the **dinfo** command.
brackets ([ ])	Indicate optional elements. You can choose none, one, or all of the options.
italic text	Indicates variable values in command syntax descriptions, new terms, file and directory names, and book titles.
quotation marks (“ ”)	Indicate the title of a chapter or section within a book.
`screen text`	Indicates data that appears on the screen. Example: `Set Bay Networks Trap Monitor Filters`
ellipsis points	Horizontal (. . .) and vertical (⋮) ellipsis points indicate omitted information.
vertical line (|)	Indicates that you enter only one of the parts of the command. The vertical line separates choices. Do not type the vertical line when entering the command. Example: If the command syntax is **show at routes** | **nets**, you enter either **show at routes** or **show at nets**, but not both.

Ordering Bay Networks Publications

To purchase additional copies of this document or other Bay Networks publications, order by part number from Bay Networks Press™ at the following numbers. You may also request a free catalog of Bay Networks Press product publications.

Phone:	1-800-845-9523
FAX - U.S./Canada:	1-800-582-8000
FAX - International:	1-916-939-1010

Acronyms

ACE	Advanced Communications Engine
ALN	Access Link Node
AN	Access Node
APPN	Advanced Peer-to-Peer Networking
ARP	Address Resolution Protocol
ASN	Access Stack Node
BCN	Backbone Concentrator Node
BGP	Border Gateway Protocol
BLN	Backbone Link Node
BLN-2	Backbone Link Node-2
BOOTP	Bootstrap Protocol
CLNP	Connectionless Network Protocol
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DLSw	data link switching
DMAP	direct memory access processor
DOS	Disk Operating System
EGP	Exterior Gateway Protocol
FDDI	Fiber Distributed Data Interface
FN	Feeder Node
FRE	fast routing engine
GAME	Gate Access Management Entity
HSSI	high-speed serial interface

ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPX	Internet Packet Exchange (Novell)
LLC	logical link control
MIB	Management Information Base
NSAP	network service access point
NVFS	Nonvolatile file system
NVRAM	Nonvolatile read access memory
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PCMCIA	Personal Computer Memory Card International Association
PPP	Point-to-Point Protocol
PPX	parallel packet express
RFC	Request for Comments
SIMM	Single Inline Memory Module
SMDS	Switched Multimegabit Data Services
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
VINES	Virtual Networking System
XNS	Xerox Networking Systems

Chapter 1
Overview of Router Management

To manage your Bay Networks routers or BNX platforms, you can

- Configure the router
- Monitor traps and events
- Monitor statistics
- Manage router files
- Monitor changes to router configuration files
- Customize router software images
- Perform administrative functions
- Track network availability and response time

Configuring the Router

You can configure your router remotely using the Configuration Manager tool in Site Manager. The Configuration Manager lets you do the following:

- Add network interfaces to the router using default values
- Customize network interfaces for your network environment
- Configure inbound and outbound traffic filters on interfaces
- Assign priorities to certain types of traffic that an interface receives
- Reconfigure the router's connection to the Technician Interface
- Specify a router's hardware configuration
- Specify administrative information about the router

To access the Configuration Manager tool, select Tools→Configuration Manager from the Site Manager main window. You must then specify the operating mode (Local File, Remote File, or Dynamic):

- Use Local File mode to create or edit a configuration file locally on the Site Manager workstation for later implementation on the router.
- Use Remote File mode if you can access the router over the network but want to implement the configuration at a later date.
- Use Dynamic mode if you can access the router over the network and want to configure the system in real time.

For more information on using the Configuration Manager, refer to *Configuring Routers*.

Monitoring Traps and Events

Two types of messages help you manage a router:

- *Trap messages* provide realtime information on the operating status of the routers running on your network. Routers using the Simple Network Management Protocol (SNMP), an industry standard, produce trap messages. You use the Trap Monitor tool in Site Manager to view these messages.
- *Event messages* also provide information on the operating status of the routers running on your network; however, event messages provide a more detailed description. You can use the Events Manager tool in Site Manager to display event messages.

  Alternatively, on UNIX workstations, you can use the Bay Networks implementation of the UNIX *syslog* facility to specify destinations for event messages. For example, you can specify a file on a remote host to which you want the *syslog* facility to forward event messages. You can then open or print the file to view the event messages.

Note: *This section focuses on using the Events Manager to display event messages. For information on using the* syslog *facility, refer to Appendix B.*

For an overview of how your routers are functioning, view the trap messages first; then view event messages for more complete descriptions of the operating status of the routers.

Table 1-1 compares trap and event messages. Refer to *Event Messages for Routers and BNX Platforms* for information on how to respond to messages.

Table 1-1. Comparing Trap Messages and Event Messages

Trap Messages	Event Messages
Realtime display	Detailed display (not in real time)
SNMP-standard	Bay Networks-specific
Usually view before event messages	Usually view after trap messages
Expensive to view (but fast)	Inexpensive to view (but slower)
Brief messages provided	Descriptive messages provided (see *Event Messages for Routers and BNX Platforms*)
No list of messages provided	List of messages and recommended responses provided (see *Event Messages for Routers and BNX Platforms*)
Use Configuration Manager to configure SNMP agent to send messages to Trap Monitor Use Trap Monitor to view and filter messages	Use Events Manager to view and filter messages
Can configure SNMP agent to send event messages to Trap Monitor	Cannot configure SNMP agent to send trap messages to Events Manager
Can save messages to ASCII file	Can save messages to ASCII file
Stored in workstation's trap history file	Stored in router's event log
Stamped with workstation's time	Stamped with router's time

Viewing Trap Messages

You view trap messages in real time using the Trap Monitor tool. To access the Trap Monitor, begin at the main Site Manager window and click on Traps or select Tools→Trap Monitor. The Trap Monitor lets you view event messages along with trap messages.

Before using the Trap Monitor, you must use the Configuration Manager to do the following:

- Specify the Internet Protocol (IP) address of your Site Manager workstation.
- Configure the SNMP agent located inside your router to send specified trap messages to the Site Manager workstation.

- If you use more than one network management application, change the trap port assigned to your Site Manager application so that Site Manager will continue to receive trap messages from the router.

The Trap Monitor tool receives trap messages from all SNMP agents on the network that are configured to send the messages. Once you configure an agent to send SNMP trap messages to your Site Manager workstation, a trap history file saves a running history of these messages. The Trap Monitor dynamically displays trap messages from the trap history file after you load the file into the Trap Monitor window.

Chapter 2 describes how to load the file into the Trap Monitor window.

Figure 1-1 shows a sample Trap Monitor window and Table 1-2 describes the window contents.

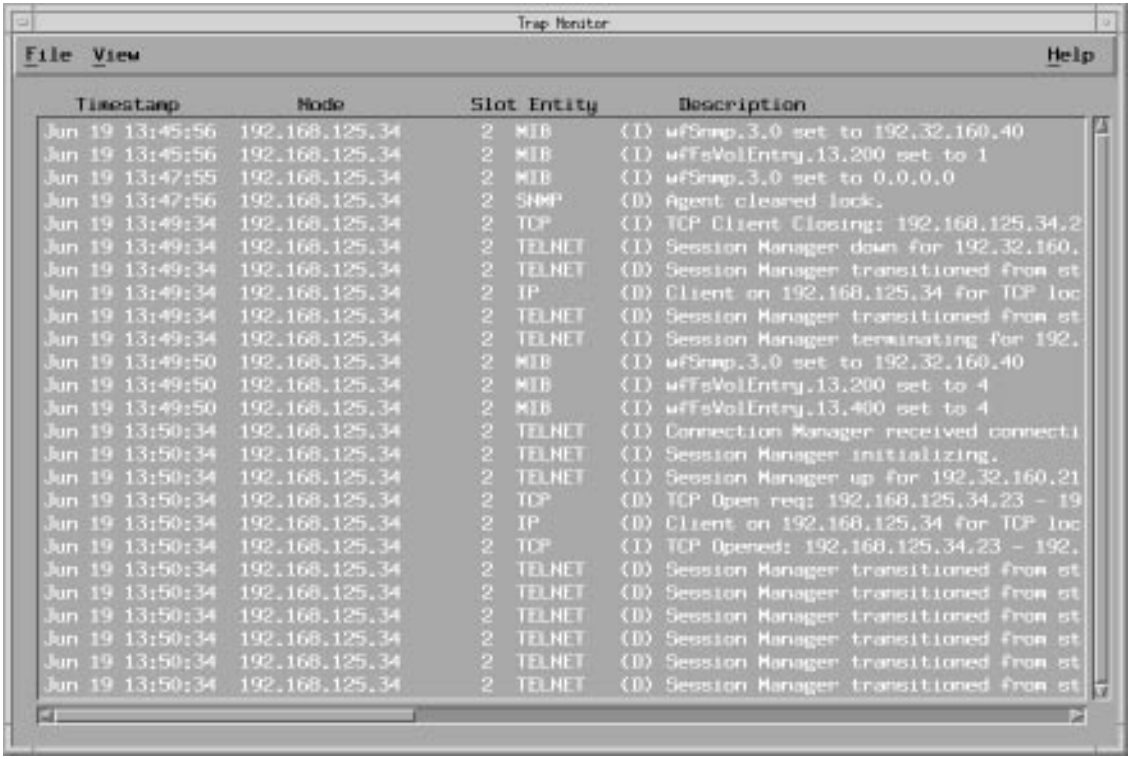
Trap Monitor
File View
Help
Timestamp Node Slot Entity Description
Jun 19 13:45:56 192.168.125.34 2 MIB (I) wfSnmp.3.0 set to 192.32.160.40
Jun 19 13:45:56 192.168.125.34 2 MIB (I) wfFsVolEntry.13.200 set to 1
Jun 19 13:47:55 192.168.125.34 2 MIB (I) wfSnmp.3.0 set to 0.0.0.0
Jun 19 13:47:56 192.168.125.34 2 SNMP (D) Agent cleared lock.
Jun 19 13:49:34 192.168.125.34 2 TCP (I) TCP Client Closing: 192.168.125.34,2
Jun 19 13:49:34 192.168.125.34 2 TELNET (I) Session Manager down for 192.32.160.
Jun 19 13:49:34 192.168.125.34 2 TELNET (D) Session Manager transitioned from st
Jun 19 13:49:34 192.168.125.34 2 IP (D) Client on 192.168.125.34 for TCP loc
Jun 19 13:49:34 192.168.125.34 2 TELNET (D) Session Manager transitioned from st
Jun 19 13:49:34 192.168.125.34 2 TELNET (I) Session Manager terminating for 192.
Jun 19 13:49:50 192.168.125.34 2 MIB (I) wfSnmp.3.0 set to 192.32.160.40
Jun 19 13:49:50 192.168.125.34 2 MIB (I) wfFsVolEntry.13.200 set to 4
Jun 19 13:49:50 192.168.125.34 2 MIB (I) wfFsVolEntry.13.400 set to 4
Jun 19 13:50:34 192.168.125.34 2 TELNET (I) Connection Manager received connecti
Jun 19 13:50:34 192.168.125.34 2 TELNET (I) Session Manager initializing.
Jun 19 13:50:34 192.168.125.34 2 TELNET (I) Session Manager up for 192.32.160.21
Jun 19 13:50:34 192.168.125.34 2 TCP (D) TCP Open req: 192.168.125.34,23 - 19
Jun 19 13:50:34 192.168.125.34 2 IP (D) Client on 192.168.125.34 for TCP loc
Jun 19 13:50:34 192.168.125.34 2 TCP (I) TCP Opened: 192.168.125.34,23 - 192.
Jun 19 13:50:34 192.168.125.34 2 TELNET (D) Session Manager transitioned from st
Jun 19 13:50:34 192.168.125.34 2 TELNET (D) Session Manager transitioned from st
Jun 19 13:50:34 192.168.125.34 2 TELNET (D) Session Manager transitioned from st
Jun 19 13:50:34 192.168.125.34 2 TELNET (D) Session Manager transitioned from st
Jun 19 13:50:34 192.168.125.34 2 TELNET (D) Session Manager transitioned from st
Jun 19 13:50:34 192.168.125.34 2 TELNET (D) Session Manager transitioned from st

Figure 1-1. Bay Networks Trap Monitor Window

Table 1-2. Trap Message Details

Item	Description
Timestamp	Date and time the Site Manager workstation received the trap message.
Node	IP address of router whose SNMP agent generated the trap message.
Slot	Slot hosting the entity that generated the trap message.
Entity	Abbreviated name of entity that generated the trap message.
Severity	Severity level of trap message: Fault, Warning, Information, Debug, or Trace. First letter is used (for example, W stands for Warning).
Description	Text describing the trap.

You can use the entity, severity, slot, and node to filter the types of trap messages you want to view in the Trap Monitor window.

The Trap Monitor tool lets you do the following:

- Save the trap messages you see in the Trap Monitor window to an ASCII file on your workstation. You can view or print the file later.
- Clear the Trap Monitor window to display only the latest messages or empty the trap history file entirely to start a new log.

You can configure the SNMP agent to send specified trap messages to the Trap Monitor window as follows:

Configuring the SNMP Agent
By category — none, generic, specific, all
By entity
By event message (entity/event code)

Note: *To save routing resources, configure the SNMP agent so that it sends only important data, such as fault, warning, and information messages.*

For more information about using the Trap Monitor, see Chapter 2.

Viewing Event Messages

You can view event messages in Site Manager using the Events Manager tool. To access the Events Manager, begin at the main Site Manager window and click on Events or select Tools→Events Manager. Each time you want to view the most current version of a router's event log, you can use the Events Manager to retrieve the event log. The Events Manager does not display event messages in real time.

The Events Manager lets you view event messages from the router whose IP address you specify in the main Site Manager window or from the Options menu in the Events Manager window.

Figure 1-2 shows a sample Events Manager window and Table 1-3 describes its contents.

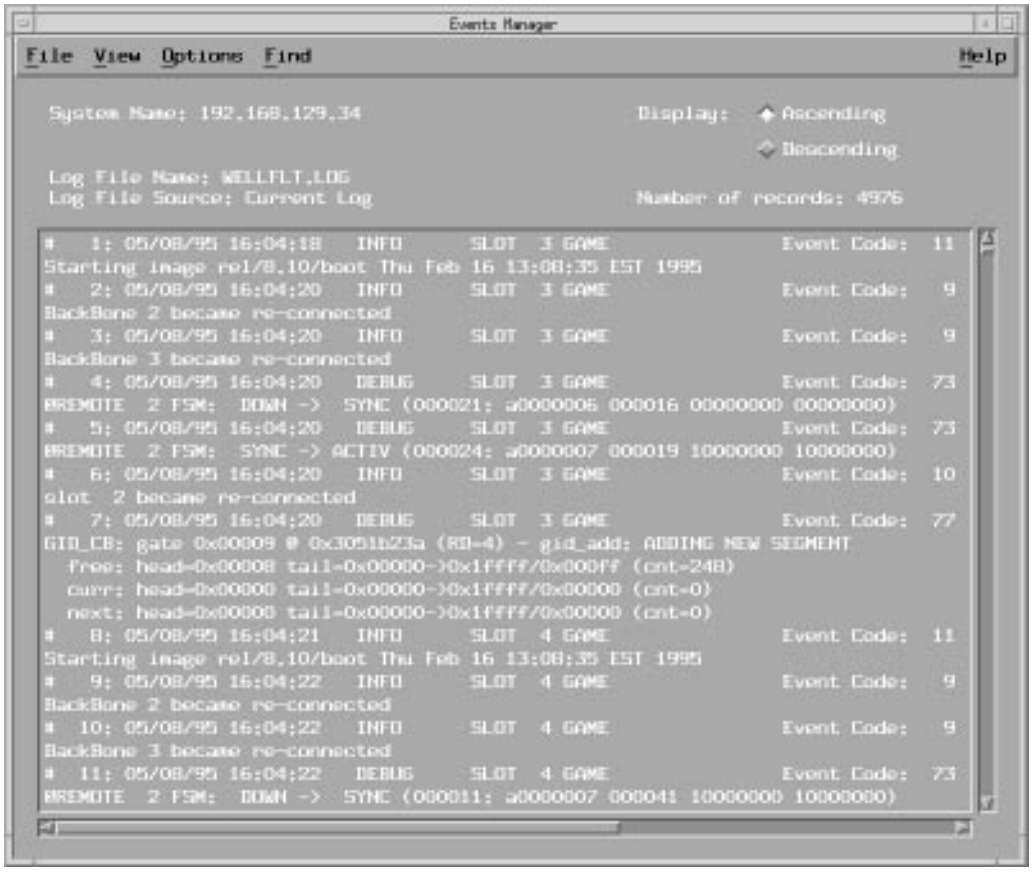
Events Manager
File View Options Find
Help
System Name: 192.168.129.34
Display: Ascending
Descending
Log File Name: WELLFLT.LOG
Log File Source: Current Log
Number of records: 4976
1: 05/08/95 16:04:18 INFO SLOT 3 GAME Event Code: 11
Starting image rel/8,10/boot Thu Feb 16 13:08:35 EST 1995
2: 05/08/95 16:04:20 INFO SLOT 3 GAME Event Code: 9
BackBone 2 became re-connected
3: 05/08/95 16:04:20 INFO SLOT 3 GAME Event Code: 9
BackBone 3 became re-connected
4: 05/08/95 16:04:20 DEBUG SLOT 3 GAME Event Code: 73
#REMOTE 2 FSM: DOWN -> SYNC (000021: a0000006 000016 00000000 00000000)
5: 05/08/95 16:04:20 DEBUG SLOT 3 GAME Event Code: 73
#REMOTE 2 FSM: SYNC -> ACTIV (000024: a0000007 000019 10000000 10000000)
6: 05/08/95 16:04:20 INFO SLOT 3 GAME Event Code: 10
slot 2 became re-connected
7: 05/08/95 16:04:20 DEBUG SLOT 3 GAME Event Code: 77
GID_CB: gate 0x00009 @ 0x3051b23a (RD=4) - gid_add: ADDING NEW SEGMENT
free: head=0x00008 tail=0x00000->0x1ffff/0x000ff (cnt=248)
curr: head=0x00000 tail=0x00000->0x1ffff/0x00000 (cnt=0)
next: head=0x00000 tail=0x00000->0x1ffff/0x00000 (cnt=0)
8: 05/08/95 16:04:21 INFO SLOT 4 GAME Event Code: 11
Starting image rel/8,10/boot Thu Feb 16 13:08:35 EST 1995
9: 05/08/95 16:04:22 INFO SLOT 4 GAME Event Code: 9
BackBone 2 became re-connected
10: 05/08/95 16:04:22 INFO SLOT 4 GAME Event Code: 9
BackBone 3 became re-connected
11: 05/08/95 16:04:22 DEBUG SLOT 4 GAME Event Code: 73
#REMOTE 2 FSM: DOWN -> SYNC (000011: a0000007 000041 10000000 10000000)

Figure 1-2. Events Manager Window

Table 1-3. Event Message Details

Detail	Description
Event number	Event's place in the event log (see the Number of Records field for the total count)
Timestamp	Date and time the event occurred, as recorded by the router
Severity	Severity level of event message
Slot	Slot hosting the entity that generated the event message
Entity	Abbreviated name of entity that generated the event message
Event code	Event code, as shown in *Event Messages for Routers and BNX Platforms*
Description	Text describing the event

You can use the router IP address, entity, severity, and slot to filter event messages in the Events Manager window.

You can use the entity and event code to look up an event message in *Event Messages for Routers and BNX Platforms*.

The Events Manager lets you do the following:

- Search for messages in the log displayed.
- Save the event messages you see in the Events Manager window to an ASCII file on your workstation. You can then view or print the file.
- Reload an event log saved in binary format back into the Events Manager window. (Storing a log on a diskette or memory card inside the router saves the log in binary format.)
- Clear the events displayed in the Events Manager window.

For more information on using the Events Manager, see Chapter 3.

Monitoring Statistics

Site Manager uses an SNMP-based polling mechanism to request the following:

- Realtime data link layer statistics providing circuit information
- Network layer statistics providing protocol information

When it receives this data, Site Manager displays the information in a statistics window. Using the Statistics Manager tool, you can do the following:

- Connect to a router
- View the Bay Networks Management Information Base (MIB)
- Display statistics screens
- Build custom statistics screens
- Edit custom statistics screens
- Add or remove statistics screens from the current screen list

To access the Statistics Manager tool, begin at the main Site Manager window and click on Statistics or select Tools→Statistics Manager. The Statistics Manager provides four tools that you can access from the Statistics Manager's Tools menu (Figure 1-3). Table 1-4 describes these tools.

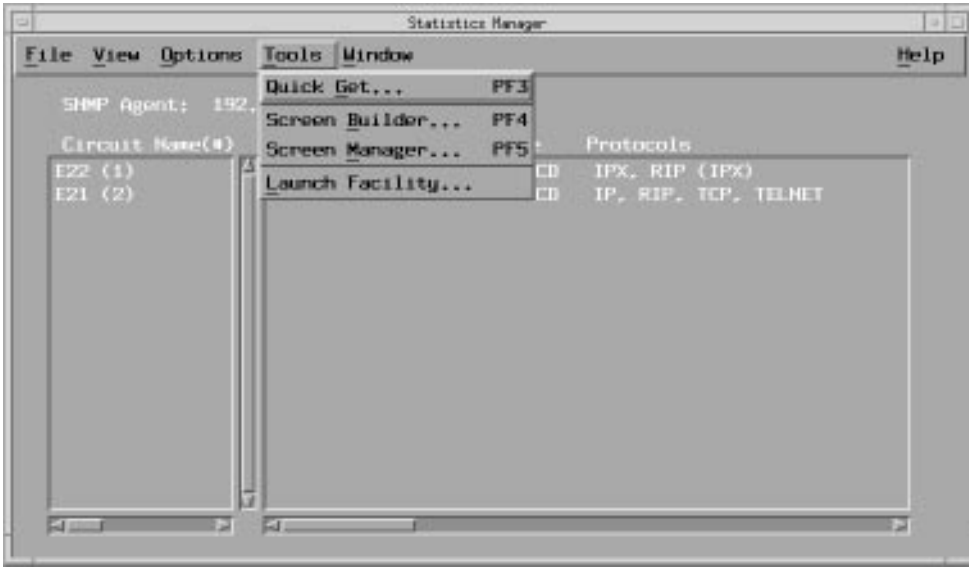

Figure 1-3. Statistics Manager Tools Menu

Table 1-4. Statistics Manager Tools

Tool	Use to
Quick Get	View objects in the Management Information Base (MIB)
Screen Builder	Design your own custom statistics screens
Screen Manager	Manage your statistics screen database and specify a current statistics screen list
Launch Facility	Select statistics screens from the current screen list and launch (or display) the screens

The following sections describe each of these tools, as well as how to get online help. Later, we describe where the Statistics Manager stores default and custom-built statistics files on your UNIX workstation or PC.

For more information about monitoring statistics, see Chapter 4. For information on file-based performance statistics (available only with BNX software), refer to *Gathering and Interpreting Performance Data (BNX Software)*.

Using the Quick Get Tool

You use Quick Get to view the MIB and retrieve instances of selected MIB objects from the router. The Bay Networks MIB is a Bay Networks proprietary database that contains the router's configuration parameters and statistics.

Quick Get includes a *MIB Browser*, which you use to scroll through the MIB and select those objects about which you want to retrieve information. Quick Get retrieves all instances of the specified MIB objects and displays the statistics in a window.

Quick Get helps you debug your network (for example, if you want to monitor MIB objects). It is also an easy way to view the MIB and decide which objects you want to include on your customized statistics screens.

Using the Screen Builder Tool

You use the Screen Builder to create custom statistics screens. The MIB Browser lets you select up to nine objects to include on the screen. For each object you select, you design how the statistics appear on the screen. The screen shows each object's statistics in a single column below a column heading.

The Screen Builder lets you specify the following:

- A name for the column heading
- The column width
- The format in which the screen displays the statistics (decimal or hexadecimal)

You can also use the Screen Builder to edit custom screens. For example, you can redefine how to display statistics, or you can add or delete objects from the screen.

Using the Screen Manager Tool

You use the Screen Manager to manage the statistics screen database and to define a *current screen list*. The database contains more than 75 default statistics screens. In addition, you can design and save up to 4,000 customized screens. The current screen list is a subset of the entire database of statistics screens — usually those you use most often. It can contain both default and custom-built screens. Note that you can display only those statistics screens that you have added to the current screen list.

Using the Launch Facility Tool

You use the Launch Facility tool to display any statistics screens that are on the current screen list. When you launch a statistics screen, Site Manager polls the router for all instances of the MIB objects specified on the screen, then it formats and displays the data in columns.

There are two types of statistics screens:

- Circuit mode: The Statistics Manager continually polls the router for statistics and updates the statistics screen with new data. You determine how often the Statistics Manager retrieves these statistics by specifying a polling rate.

- Table mode: The Statistics Manager retrieves statistics from the router only once — when you launch the screen. You must refresh the screen each time you want to update it with new data.

Using Online Help

Site Manager provides online help for each Statistics Manager tool. To get help, click on Help at the bottom of the screen. To exit the Help window, click on OK.

Locating Statistics Files

Depending on whether you load Site Manager on a UNIX or DOS computer, the Statistics Manager stores all statistics screen files in one of the following directories.

Platform	Default Screen Directory	Custom Screen Directory
UNIX	*/usr/wf/lib/.wfscrns*	*$(HOME)/.wfscrns*
DOS	*\wf\lib\wfscrns*	*\wf\wfscrns*

For more information on using the Statistics Manager, refer to Chapter 4.

Managing Router Files

You can display a list of the system files stored on a Bay Networks router's active volume using the Router Files Manager tool. The Router Files Manager lets you

- Display the files on all disk volumes in a Bay Networks router
- Transfer and copy files between volumes on a Bay Networks router's disk and between the router and the Site Manager workstation
- Delete files from a Bay Networks router's disk volume
- Compact Bay Networks memory cards
- Partition the nonvolatile file system (NVFS) on Bay Networks Access Node (AN™) or Access Stack Node (ASN™) routers

To access the Router Files Manager, begin at the main Site Manager window and click on Files or select Tools→Router Files Manager. For more information about using the Router Files Manager, refer to Chapter 5.

Monitoring Changes to Router Configuration Files

Two features are available for you to track changes to router configuration files:

- The Report Generator tool
- The Audit Trail feature

The Report Generator tool translates the router's binary configuration file to an ASCII file. You can use any standard text editor to view and print the file. You can also use source-comparison utilities to compare one report with another to detect configuration changes. To access the Report Generator tool, select Tools→Report Generator from the Site Manager main window.

In organizations where network managers at branch locations share router management responsibilities, central administrators can use audit trail logs to monitor configuration changes. An audit trail log is an ASCII file that describes the changes made to a router configuration file. Each router you audit has its own audit trail log file. Whenever someone changes a router configuration file, the audit trail feature (if enabled for that router) appends the changes to the audit trail log.

Note: *The Audit Trail feature keeps track of router configuration changes made in remote mode or dynamic mode only. The feature does not track changes made in local mode or those made using the Technician Interface.*

With audit trail logging enabled, when you configure the router in remote mode, Site Manager does the following, once you save your configuration changes:

- Transfers the configuration file to the router, as usual
- Creates the audit trail log file (if it doesn't already exist)
- Appends the configuration changes to the audit trail log file

If you configure the router in dynamic mode, Site Manager does the following each time an SNMP SET occurs:

- Updates the configuration on the router.
- Logs the SET to the audit trail log file. Site Manager creates the audit trail log file (if it does not already exist) and appends the changes to the file.

Note: *To prevent an audit trail log file from becoming too large, you should periodically delete old information in it or delete the file itself.*

You can configure the Audit Trail feature to send you (and other network managers) a copy of the audit trail log file whenever Site Manager updates it with new information. For routers configured in dynamic mode, the Audit Trail feature sends the log file after every tenth SNMP set.

For more information on using the Report Generator tool and the Audit Trail feature, refer to Chapter 6.

Customizing Router Software Images

Site Manager provides a tool, the Image Builder, that lets you customize the *router software images* you receive from Bay Networks. A router software image is a group of executable files that operates the protocols on your network in conjunction with a Bay Networks router. You can do the following to modify a router software image:

- Remove a protocol that you do not use. For example, you might want to remove protocols to make more space available on the media that contains the router software image. Alternatively, you can add protocols that you inadvertently removed.
- Replace an existing image with an entirely new one.

Note: *The Image Builder is not supported by BNX Software.*

To access the Image Builder, select Tools→Image Builder. For more information on using the Image Builder tool, refer to *Modifying Software Images for Routers*.

Performing Administrative Functions

You can perform the following administrative tasks from Site Manager:

- Booting (warm-starting) the router
- Resetting (warm-starting) a single processor module in the router
- Clearing the router's event log
- Setting the router's date and time
- Testing the router's connection to a remote device on the network using one of the following protocols: APPN, IP, IPX, OSI, VINES, or AppleTalk
- Configuring the kernel; that is, reallocating the global and local memory on FRE2 and ACE32 processor modules, Access Nodes, and Access Feeder Nodes

You can perform these tasks using the Site Manager Administration menu (Figure 1-4).

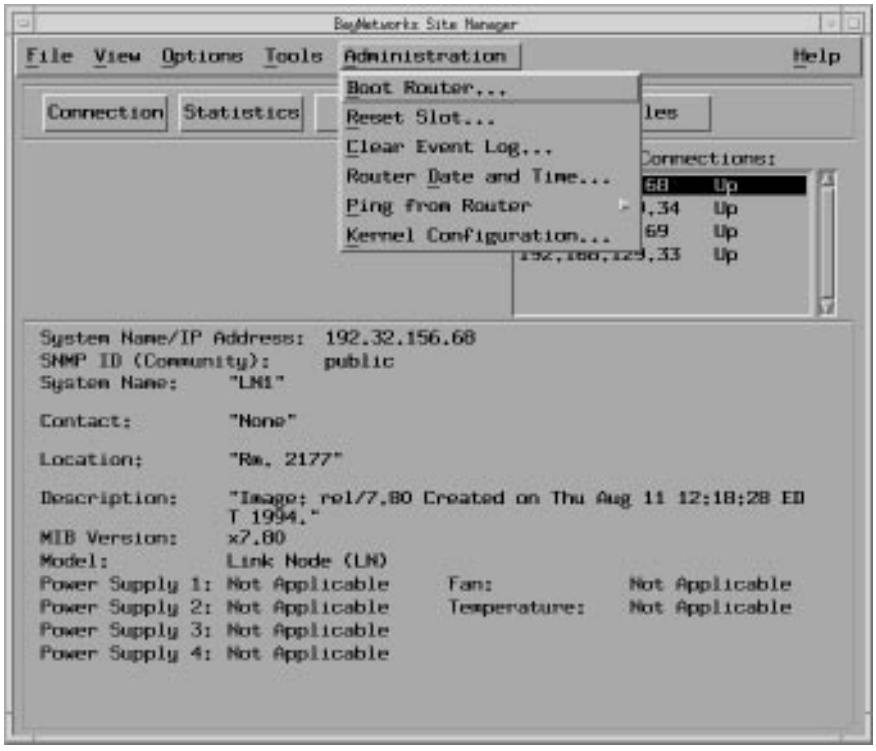

Figure 1-4. Site Manager Administration Menu Window

For more information about using each of the administrative functions, refer to Chapter 7.

Tracking Network Availability and Response Time

You can track network availability and response time using the Ping MIB. The Ping MIB is a group of tables that stores the following information for one or more ping requests:

- General ping information, such as the address you want to ping, whether you want to use trace routing and source routing, and the frequency of the ping.
- Trace route data that shows the IP addresses the ping went through to reach its destination.

- Source route data, which contains the IP addresses that you want the ping to go through instead of those in the routing table.
- History data about previous pings that you chose to initiate at specific intervals. See Chapter 8 for information on setting ping intervals.

To use the Ping MIB, you must first define the IP addresses that you want to ping. You can enter the addresses of routers, host computers, or any device on the network. The Ping MIB stores the results of the ping requests. You can then monitor those results using the Statistics Manager in Site Manager. You might also create your own application to query the Ping MIB, analyze the data, and generate reports of the information. You can also use such applications as IBM NetView/6000, SunNet Manager, and HP OpenView to work with the Ping MIB.

For more information on using the Ping MIB, refer to Chapter 8.

Keeping a Log

You should make several copies of the log on the next page to organize your management files. Keep the log in a handy place near your Site Manager workstation. Use this log to list the filenames and directories of all your configuration files, trap history files, and event logs.

LOG

Filename	Directory	Description	Date

Chapter 2
Using the Trap Monitor

For general information about monitoring traps, see “Monitoring Traps and Events” in Chapter 1. For specific information about using buttons, windows, and other Site Manager features, refer to *Using Site Manager Software.*

Use the Trap Monitor to do the following:

- Display the trap history file
- Filter trap messages
- Clear the Trap Monitor window
- Clear the trap history file
- Save trap messages

Connecting to a Router

Before you can use the Trap Monitor tool, you must configure the Simple Network Management Protocol (SNMP) agent inside the router to send specified trap messages to the Trap Monitor. To do this, you must first connect to the router as follows:

1. **From the Bay Networks Site Manager window, select Options→ Connections.**

   The Router Connection Options window appears (Figure 2-1).

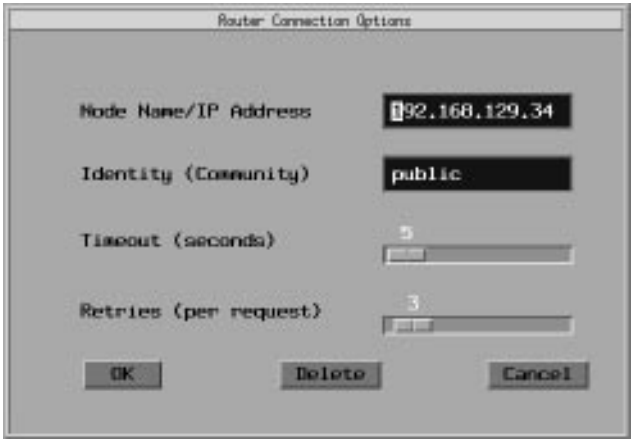

Figure 2-1. Router Connection Options Window

2. **In the Node Name/IP Address field, type the IP address of the router you want to configure. Then click on OK.**

The Bay Networks Site Manager window displays the router's system information.

Configuring the Router's SNMP Agent

You must configure the SNMP agent in a router such that it will

- Recognize your Site Manager workstation as a valid SNMP manager
- Send specified trap messages to your Site Manager workstation

To configure the SNMP agent, use the Configuration Manager tool, which you also use to

- Enable the SNMP agent on the router
- Save the result of your configuration entries on the router

This section explains briefly how to accomplish these tasks. For more information on how to customize traps a router sends, refer to *Configuring SNMP, BOOTP, DHCP, and RARP Services*.

Identifying Site Manager as an SNMP Manager

To configure the router's SNMP agent to send trap messages to your Site Manager workstation, you must first tell the router to recognize your Site Manager workstation as a valid SNMP manager.

1. **From the Bay Networks Site Manager window, select Tools→Configuration Manager. Then select Local File, Remote File, or Dynamic mode.**

   The Configuration Manager window appears (Figure 2-2).

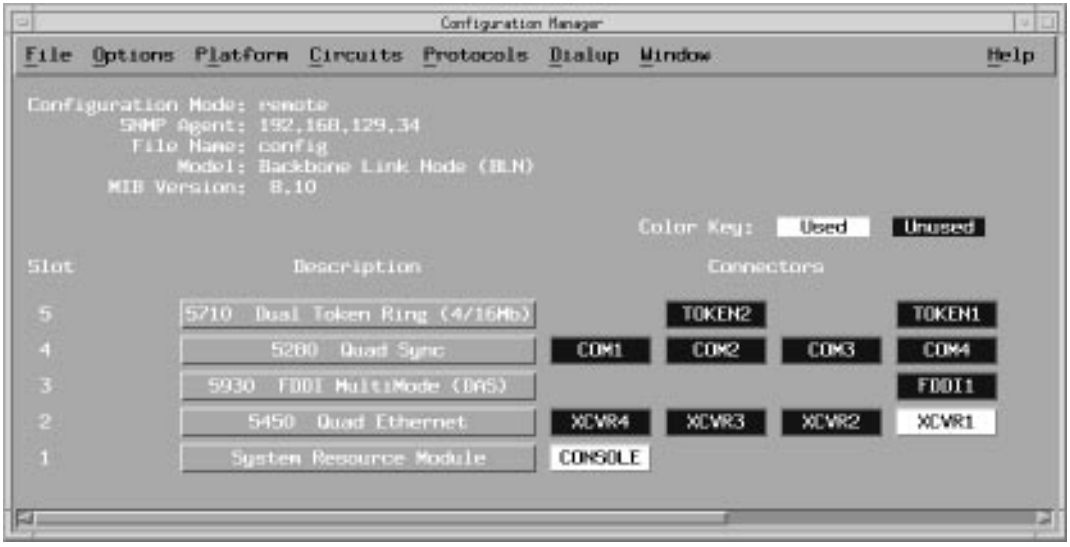

Figure 2-2. Configuration Manager Window

2. **From the Configuration Manager window, select Protocols→IP→SNMP→Communities.**

   The SNMP Community List window appears (Figure 2-3).

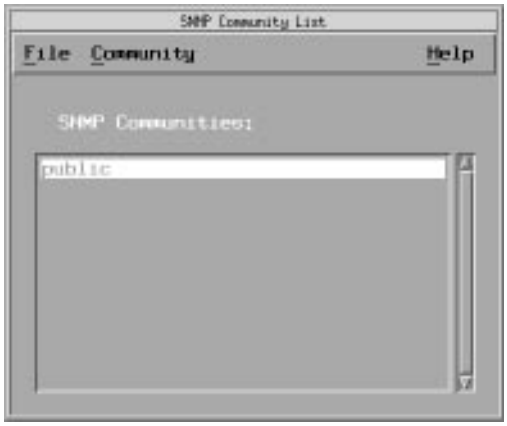

Figure 2-3. SNMP Community List Window

3. **From the SNMP Community List window, select Community→Managers.**

   The SNMP Manager List window appears (Figure 2-4).

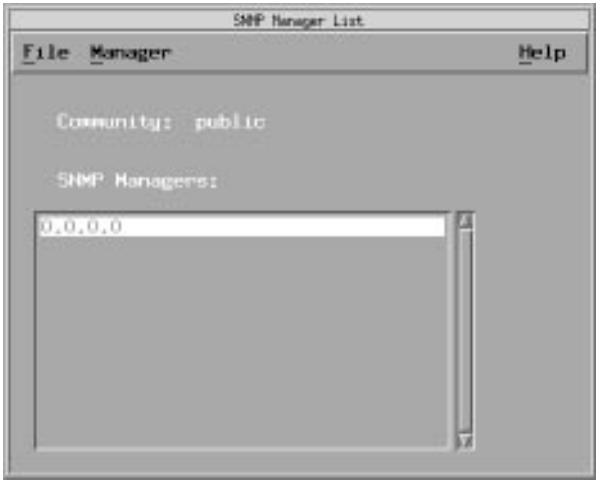

Figure 2-4. SNMP Manager List Window

4. **From the SNMP Manager List window, select Manager→Add Manager.**

The Add SNMP Manager window appears (Figure 2-5).

Figure 2-5. Add SNMP Manager Window

5. **Type the IP address of your Site Manager workstation. Then click on OK.**

   The SNMP Manager List window displays your workstation's IP address.

6. **Select File→Exit in the SNMP Manager List window.**

   You return to the SNMP Community List window.

7. **Select File→Exit in the SNMP Community List window.**

   You return to the Configuration Manager window.

8. **Save this configuration to a file and volume on the router.**

Saving a Configuration

To save a configuration to a file and volume on the router, select File→Save or File→Save As from the Configuration Manager window. Exiting from the Configuration Manager window also prompts you to save a configuration. Specify the filename and router volume, then select Save. Note the name and router volume you specified.

Refer to *Configuring Routers* or *Configuring Customer Access and Trunks (BNX Software)* for more information on using the Configuration Manager tool.

Running Multiple Network Management Applications

If you are running another network management application (besides Site Manager) on your workstation, you must configure Site Manager to receive trap messages via another port on your Site Manager workstation. This is necessary for the following reasons:

- The router can only send trap messages to one network management application at a time.
- Only one application can map to a port at a time.

Note: *By default, a network management application installed on your workstation binds to UDP (User Datagram Protocol) Port 162. This port is dedicated to receiving SNMP traps from the SNMP agent. Since Site Manager is the preferred network management application for receiving trap messages, we recommend that, when running another manager, you configure Site Manager to bind to an alternative UDP port where Site Manager can continue to receive trap messages.*

To configure the SNMP agent to send trap messages to Site Manager via a different port, follow these steps:

1. **From the Configuration Manager window, select Protocols→IP→SNMP→Communities.**
2. **From the SNMP Community List window that appears, select Community→Managers.**
3. **From the SNMP Manager List window, select Manager→Edit Manager.**

   The Trap Port and Trap Types window appears with the default value 162 (Figure 2-6).

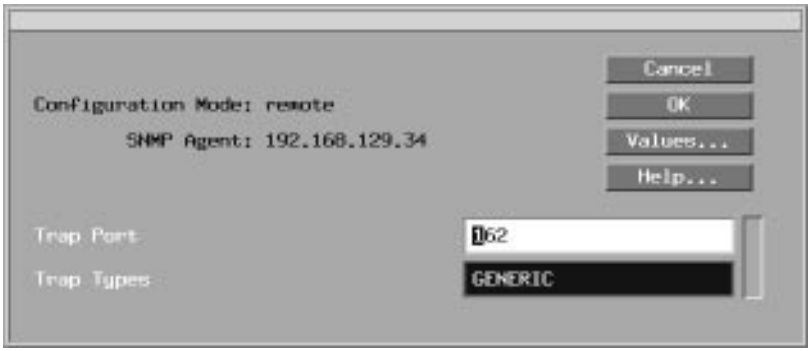

Figure 2-6. Trap Port and Trap Types Window

4. **To select a port number, use the Values button or type a port number in the Trap Port field.**

   You can enter any port number on your Site Manager workstation, as long as another application is not using that port.

5. **Click on OK in the Trap Port and Trap Types window.**

6. **Save this configuration to a file and volume on the router.**

   For information, see the previous section, "Saving a Configuration."

7. **Exit Site Manager by selecting File→Exit from the Bay Networks Site Manager window.**

8. **Restart Site Manager using either the UNIX or DOS commands shown in Table 2-1.**

Table 2-1. Restarting Site Manager on a New Port

Platform	Steps
UNIX	1.Open a command line window. 2.Enter **wfsm -e** *<port number>* at the prompt.
DOS	1.Start the Windows environment. The Program Manager window appears. 2.Double-click on the Site Manager program group from the Program Manager window. 3.Select the PC/Site Manager icon in the Site Manager program group. 4.Select File→Properties. 5.Add **-e** *<port number>* to the end of the command line. 6.Double-click on the PC/Site Manager icon.

Note: *You must specify the new port number every time you restart Site Manager.*

Configuring Traps Sent by a Router

You can specify by category, entity, or event the types of trap messages you want a router to send to your Site Manager workstation.

Specifying Traps by Category

You can configure a router to send

- All traps
- Generic traps
- Specific traps
- No traps

To specify the trap types you want to receive at your workstation, follow these steps:

1. **From the Configuration Manager window, select Protocols→IP→SNMP→Communities.**

2. **From the SNMP Community List window that appears, select Community→Managers.**

3. **From the SNMP Manager List window that appears, select Manager→Edit Manager.**

   The Trap Types and Trap Port window appears with the default value GENERIC in the Trap Types field (Figure 2-7).

Figure 2-7. Specifying a Trap Category

4. **Click in the Trap Types field. Click on Values and select an option in the Values Selection window. Then click on OK in the Values Selection window.**

   Table 2-2 describes the different trap types.

Table 2-2. Categories of Traps

Category	Description
NONE	Prohibits the SNMP agent from transmitting traps to this manager.
GENERIC	Configures the agent to transmit well-defined SNMP traps (cold-start, warm-start, and authentication failure traps). The agent is automatically enabled to send cold-start and warm-start traps. However, you must enable the Authentication Failure Trap parameter if you want the agent to transmit authentication failure traps as well.

(continued)

Table 2-2. Categories of Traps *(continued)*

Category	Description
SPECIFIC	Configures the agent to transmit all enabled trap message types (fault, warning, debug, information, and trace traps) from the protocol entities on your network.
ALL	Configures the agent to transmit cold-start and warm-start traps, as well as all other enabled traps (authentication failure, fault, warning, debug, information, and trace traps).

Note: *You will usually want to select GENERIC or SPECIFIC when you configure the SNMP agent to send traps. These options minimize the agent's use of router resources.*

5. **Click on OK in the Trap Port and Trap Types window.**
6. **Save this configuration to a file and volume on the router.**

Note: *If you select SPECIFIC, you must further specify by entity the kinds of trap messages you want the SNMP agent to send to your workstation. Proceed to the section "Specifying Traps by Entity."*

Specifying Traps by Entity

If you configure an SNMP agent to send SPECIFIC trap types to your Site Manager workstation, you must specify which protocols (entities) will send which trap types (fault, warning, information, debug, or trace) to your workstation. Proceed as follows:

1. **From the Configuration Manager window, select Protocols→IP→SNMP→Trap Configuration→Interfaces.**

   The Trap Configuration window appears (Figure 2-8).

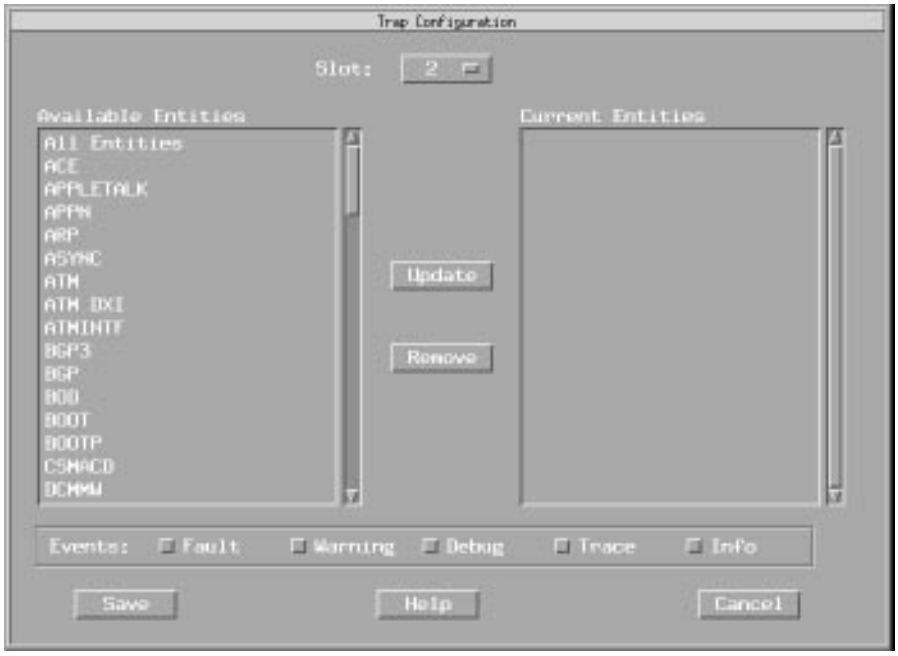

Figure 2-8. Trap Configuration Window

2. **Select the appropriate slot.**
3. **Select an entity whose trap messages you want to receive at your Site Manager workstation.**
4. **Select the severity levels for that entity's trap messages.**
5. **Click on Update.**

   The entity and severity levels are added to the Current Entities field.
6. **Repeat Steps 2 through 5 for every entity whose trap messages you want to receive at your Site Manager workstation. Then click on Save.**
7. **Save this configuration to a file and volume on the router.**

The entities you select will now send the trap types you selected to your workstation.

Specifying Traps by Event Type

You can configure a router to always (or never) send trap messages that you designate by their unique entity code and event number. Proceed as follows:

1. **From the Configuration Manager window, select Protocols→IP→SNMP→Trap Configuration→Exceptions.**

   The Traps Exceptions Lists window appears (Figure 2-9).

Figure 2-9. Traps Exceptions Lists Window

2. **To add an event message to the list of trap messages sent to your router, click on Add in the Traps Exceptions Lists window.**

   The Add Trap window appears (Figure 2-10).

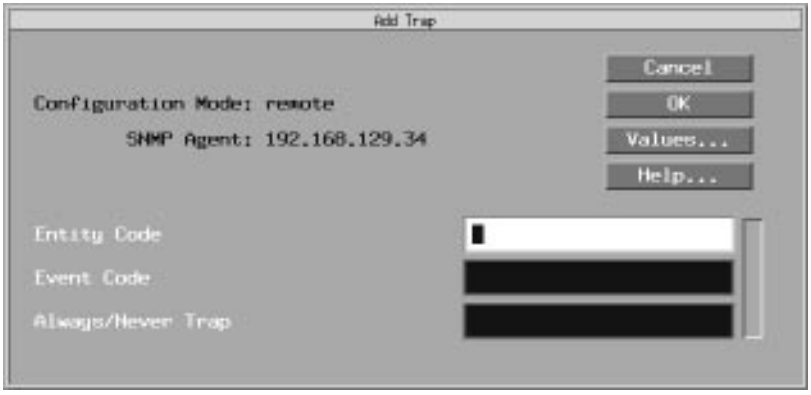

Figure 2-10. Add Trap Window

3. **To determine which Entity Code and Event Code values to specify, refer to** *Event Messages for Routers and BNX Platforms.*

4. **Click on Values to enter values in the three fields shown in the Add Trap window.**

   Table 2-3 shows the values you should enter.

Table 2-3. Entering Values in the Add Trap Window

Field	Value
Entity Code	Enter a value between 0 and 61.
Event Code	Enter a value between 0 and 255.
Always/Never Trap	Enter ALWAYS.

5. **Click on OK in the Add Trap window.**

   The entity's event type appears in the Traps Exceptions Lists window (Figure 2-11).

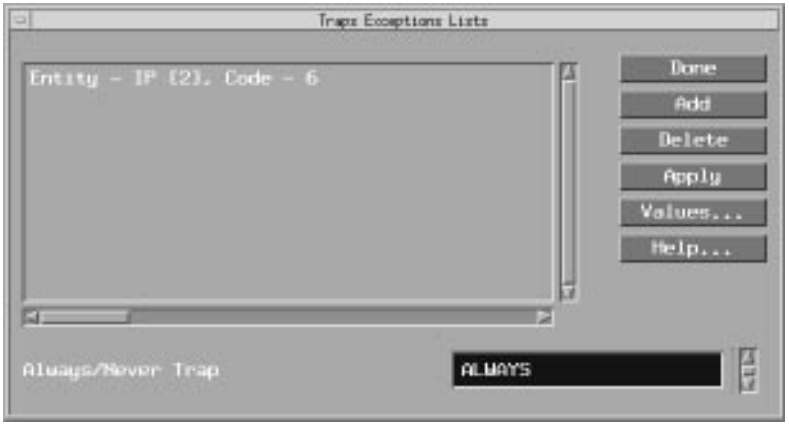

Figure 2-11. Traps Exceptions Lists Window

You have now specified a particular entity's event message to be sent to your Site Manager workstation's Trap Monitor.

6. **Repeat this procedure for every entity's event message you want sent to the Trap Monitor.**
7. **Click on Apply, and then click on Done.**
8. **Save this configuration to a file and volume on the router.**

You have now configured the SNMP agent inside each specified router to send event messages, along with trap messages, to your Site Manager workstation's Trap Monitor.

Enabling an SNMP Agent

By default, the SNMP agent is always enabled. However, if the agent is disabled at some point, you will have to enable it. To enable an SNMP agent to send trap messages to your Site Manager workstation, follow this procedure:

1. **From the Configuration Manager window, select Protocols→IP→SNMP→Global.**

   The Edit SNMP Global Parameters window appears (Figure 2-12).

Figure 2-12. Edit SNMP Global Parameters Window

2. **Click on Values and select Enable from the Values Selection window (Figure 2-13). Then click on OK.**

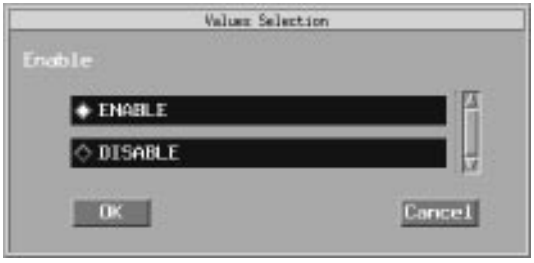

Figure 2-13. Values Selection Window

3. **Click on OK in the Edit SNMP Global Parameters window to save your changes and exit the window.**
4. **Save this configuration to a file and volume on the router.**

You have now configured this router's SNMP agent to send trap messages to your Site Manager workstation.

Viewing Trap Messages

Your Site Manager workstation receives all types of trap messages that routers in your network are configured to send. However, the Trap Monitor tool lets you choose, from all trap messages received by the workstation, which traps you want to view in the Trap Monitor window. You can filter trap message types by severity or by IP address (using address filters).

The next section describes how to configure the Trap Monitor to receive trap messages from routers throughout your network.

Using the Trap Monitor

The Trap Monitor tool lets you filter and view trap messages. Before you use the Trap Monitor tool to view trap messages, configure the SNMP agent in each router to send trap messages, as described earlier. The agent running in the router sends only the trap types that you enable in the router configuration. The Trap Monitor running in your Site Manager workstation subsequently filters and displays a subset of all the trap messages it receives from routers in your network.

Note: *If you configure your routers to send traps, do not exit the Trap Monitor window. Otherwise, the routers log this message:*

```
ICMP Destination unreachable
```

Displaying the Trap History File

The trap history file contains trap messages that you specified be sent to your Site Manager workstation. The Trap Monitor dynamically displays trap messages from this file after you load the trap history file into the Trap Monitor window.

Use the Load History File feature to display all trap messages since you last cleared the history file.

1. **From the main Site Manager window, click on Traps or select Tools→Trap Monitor.**

   The Trap Monitor window appears.

2. **From the Trap Monitor window, select File→Load History File.**

   The Trap Monitor window displays incoming trap messages, along with trap messages logged since you last cleared the history file.

Figure 2-14 shows the Trap Monitor window with messages.

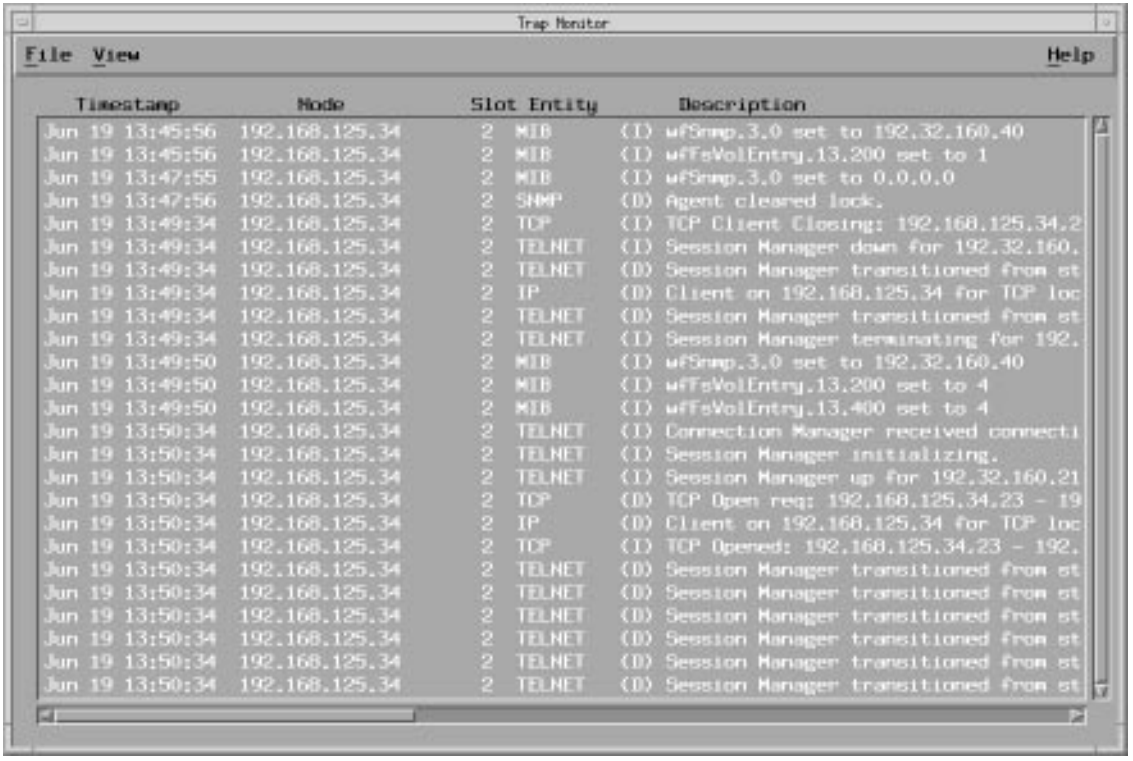
Trap Monitor
File View Help
Timestamp Node Slot Entity Description
Jun 19 13:45:56 192.168.125.34 2 MIB (I) wfSnmp.3.0 set to 192.32.160.40
Jun 19 13:45:56 192.168.125.34 2 MIB (I) wfFsVolEntry.13.200 set to 1
Jun 19 13:47:55 192.168.125.34 2 MIB (I) wfSnmp.3.0 set to 0.0.0.0
Jun 19 13:47:56 192.168.125.34 2 SNMP (D) Agent cleared lock.
Jun 19 13:49:34 192.168.125.34 2 TCP (I) TCP Client Closing: 192.168.125.34,2
Jun 19 13:49:34 192.168.125.34 2 TELNET (I) Session Manager down for 192.32.160.
Jun 19 13:49:34 192.168.125.34 2 TELNET (D) Session Manager transitioned from st
Jun 19 13:49:34 192.168.125.34 2 IP (D) Client on 192.168.125.34 for TCP loc
Jun 19 13:49:34 192.168.125.34 2 TELNET (D) Session Manager transitioned from st
Jun 19 13:49:34 192.168.125.34 2 TELNET (I) Session Manager terminating for 192.
Jun 19 13:49:50 192.168.125.34 2 MIB (I) wfSnmp.3.0 set to 192.32.160.40
Jun 19 13:49:50 192.168.125.34 2 MIB (I) wfFsVolEntry.13.200 set to 4
Jun 19 13:49:50 192.168.125.34 2 MIB (I) wfFsVolEntry.13.400 set to 4
Jun 19 13:50:34 192.168.125.34 2 TELNET (I) Connection Manager received connecti
Jun 19 13:50:34 192.168.125.34 2 TELNET (I) Session Manager initializing.
Jun 19 13:50:34 192.168.125.34 2 TELNET (I) Session Manager up for 192.32.160.21
Jun 19 13:50:34 192.168.125.34 2 TCP (D) TCP Open req: 192.168.125.34,23 - 19
Jun 19 13:50:34 192.168.125.34 2 IP (D) Client on 192.168.125.34 for TCP loc
Jun 19 13:50:34 192.168.125.34 2 TCP (I) TCP Opened: 192.168.125.34,23 - 192.
Jun 19 13:50:34 192.168.125.34 2 TELNET (D) Session Manager transitioned from st
Jun 19 13:50:34 192.168.125.34 2 TELNET (D) Session Manager transitioned from st
Jun 19 13:50:34 192.168.125.34 2 TELNET (D) Session Manager transitioned from st
Jun 19 13:50:34 192.168.125.34 2 TELNET (D) Session Manager transitioned from st
Jun 19 13:50:34 192.168.125.34 2 TELNET (D) Session Manager transitioned from st
Jun 19 13:50:34 192.168.125.34 2 TELNET (D) Session Manager transitioned from st

Figure 2-14. Trap Monitor Window

You can scroll through the trap messages using the scroll bars on the bottom and right side of the window.

Filtering Trap Messages

The Trap Monitor gives you two viewing options:

- Select Trap Types
- Set Address Filters

Using these options, you can filter by severity or by router IP address all trap messages that the Trap Monitor tool receives. The Trap Monitor displays only those trap types that you specify.

Filtering by Severity

To filter trap messages by type (fault, warning, information, debug, or trace), proceed as follows:

1. **From the Trap Monitor window, select View→Select Trap Types.**

   The Selected Trap-Types window appears (Figure 2-15).

Figure 2-15. Selected Trap-Types Window

2. **Select the trap types you want the Trap Monitor to display, then click on OK.**

Note: *The fault, warning, and information types are usually the most useful types to select.*

The Trap Monitor window displays only those trap messages that you specify. Refer to "Clearing the Trap Monitor Window," later in this chapter, to learn how to remove unwanted messages from the window.

Filtering by Router IP Address

Filtering messages by IP source address specifies which routers' trap messages you want to appear in the Trap Monitor window. Specifying a full IP address causes the Trap Monitor to show trap messages that originate from the SNMP agent at that address only.

Specifying a partial IP address causes the Trap Monitor to show trap messages from all router SNMP agents that have the same partial IP address that you specify in the address filters window.

To configure an address filter from the Trap Monitor window, follow these steps:

1. **Select View→Set Address Filters.**

   The Address Filters window appears (Figure 2-16).

Figure 2-16. Address Filters Window

   A default address filter of 0.0.0.0 causes the Trap Monitor to display trap messages from all Bay Networks routers that you configure to send trap messages to your Site Manager workstation.

   The default address filter entry, 255.255.255.255, is merely a placeholder for an IP address that you choose to enter.

2. **In the Address Filters window, specify one or more IP addresses and/or address filters.**

   You can enter as many as five complete IP addresses or address filters. The remaining fields must display the placeholder IP number 255.255.255.255.

   Figure 2-17 shows a sample Address Filters window.

Figure 2-17. Sample Address Filters Window

With this configuration, you can view trap messages from all routers with IP addresses starting with 128. and 192.32., along with those from the router at IP address 140.250.200.1.

3. **Click on Save.**

Once you save the filter entries, the Trap Monitor displays trap messages only from those routers with an IP address that matches the value you specify in the Address Filters window.

Clearing the Trap Monitor Window

To clear the Trap Monitor window, select View→Clear Window. The Trap Monitor clears the window of all trap messages.

Since the system constantly updates the trap history file, new trap messages appear right away.

Clearing the Trap History File

The trap history file can hold only a fixed number of messages. When it reaches its limit, it starts overwriting the log at the beginning. The Trap Monitor lets you empty the current trap history file so that you can start a new log of trap messages.

From the Trap Monitor window, select File→Clear History File.

The Trap Monitor updates the trap history file and begins immediately to store new trap messages.

Saving Trap Messages

The Trap Monitor lets you save the traps currently displayed in the Trap Monitor window to an ASCII file on your Site Manager workstation. You can later view, edit, or print this file.

To save trap messages to an ASCII file, proceed as follows:

1. **From the Trap Monitor window, select File→Save Traps.**

   The Trap Monitor prompts you to name the file (Figure 2-18).

Figure 2-18. Saving Traps to a File

2. **Type a directory and filename; then click on Save.**

   The system saves the log to an ASCII file on your computer. (If you do not specify a directory, the system saves the file to your local directory.) The Trap Monitor window reappears.

Note: *You cannot reload an ASCII file back into the Trap Monitor.*

Chapter 3
Monitoring Router Events

For general information about monitoring events, see “Monitoring Traps and Events” in Chapter 1. For specific information about using buttons, windows, and other Site Manager features, refer to *Using Site Manager Software*.

Use the Events Manager to do the following:

- Display event logs
- Filter event messages
- Search for an event message
- Refresh the Events Manager window
- Clear the Events Manager window
- Save event messages
- Clear the current event log

For information on using the *syslog* utility on a UNIX workstation to monitor events, refer to Appendix B.

Connecting to a Router

When you want to view a router’s event messages, you can connect to the router from either the main Site Manager window or the Events Manager window. To connect to a router through the Events Manager, begin at the main Site Manager window and proceed as follows:

1. **Click on Events or select Tools→Events Manager.**

   The Events Manager window appears.

2. **From the Events Manager window, select Options→Connections.**

   The Router Connection Options window appears (Figure 3-1).

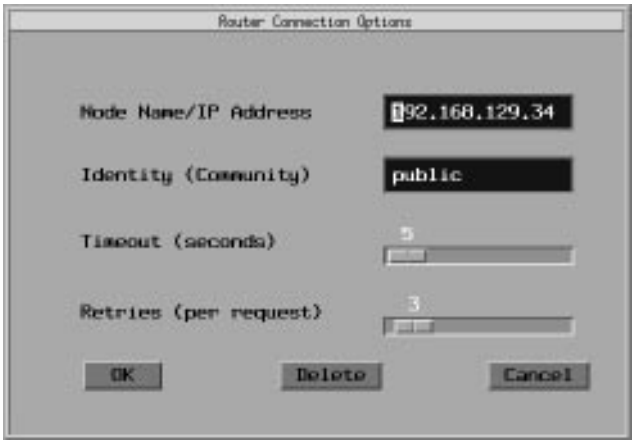

Figure 3-1. Router Connection Options Window

3. **In the Node Name/IP Address field, type the IP address of the desired router. Then click on OK.**

The Events Manager window displays the specified IP address.

Displaying Event Logs

You must load an event log into the Events Manager window before event messages will appear there. There are three types of event logs:

- Current: the log in the router's memory
- Remote: the log on the router's Flash memory card or diskette
- Local: the log transferred and saved (in binary format) to the Site Manager workstation

When you retrieve an event log file using Site Manager, you are using the Trivial File Transfer Protocol (TFTP) to transfer this file from the router's memory to the Site Manager workstation.

Displaying the Current Log

The current log is the temporary log file in the router's memory.

Before you display these event messages, you must first connect to the router whose event log you want to view. Then, to display the current log in the router's memory, select File→Get Current Log File from the Events Manager window.

Event messages will now appear in the Events Manager window (Figure 3-2), along with fields displaying the following information:

- `WELLFLT.LOG` in the Log Filename field
- `Current Log` in the Log File Source field
- Total events in the Number of Records field

For suggested responses to specific event messages, refer to *Event Messages for Routers and BNX Platforms*.

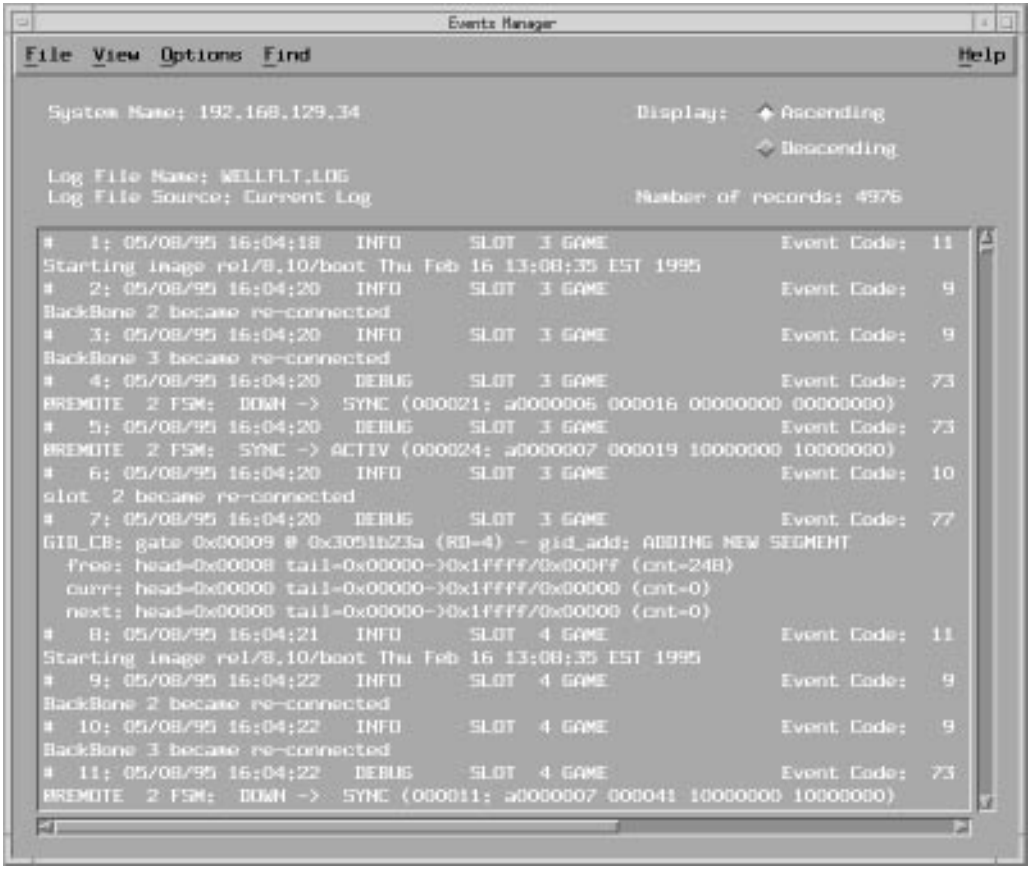
Events Manager
File View Options Find Help
System Name: 192.168.129.34
Display: Ascending
Descending
Log File Name: WELLFLT.LOG
Log File Source: Current Log
Number of records: 4976
1: 05/08/95 16:04:18 INFO SLOT 3 GAME Event Code: 11
Starting image rel8.10/boot Thu Feb 16 13:08:35 EST 1995
2: 05/08/95 16:04:20 INFO SLOT 3 GAME Event Code: 9
BackBone 2 became re-connected
3: 05/08/95 16:04:20 INFO SLOT 3 GAME Event Code: 9
BackBone 3 became re-connected
4: 05/08/95 16:04:20 DEBUG SLOT 3 GAME Event Code: 73
#REMOTE 2 FSM: DOWN -> SYNC (000021: a0000006 000016 00000000 00000000)
5: 05/08/95 16:04:20 DEBUG SLOT 3 GAME Event Code: 73
#REMOTE 2 FSM: SYNC -> ACTIV (000024: a0000007 000019 10000000 10000000)
6: 05/08/95 16:04:20 INFO SLOT 3 GAME Event Code: 10
slot 2 became re-connected
7: 05/08/95 16:04:20 DEBUG SLOT 3 GAME Event Code: 77
GID_CB: gate 0x00009 @ 0x3051b23a (RD=4) - gid_add: ADDING NEW SEGMENT
free: head=0x00008 tail=0x00000->0x1ffff/0x000ff (cnt=248)
curr: head=0x00000 tail=0x00000->0x1ffff/0x00000 (cnt=0)
next: head=0x00000 tail=0x00000->0x1ffff/0x00000 (cnt=0)
8: 05/08/95 16:04:21 INFO SLOT 4 GAME Event Code: 11
Starting image rel8.10/boot Thu Feb 16 13:08:35 EST 1995
9: 05/08/95 16:04:22 INFO SLOT 4 GAME Event Code: 9
BackBone 2 became re-connected
10: 05/08/95 16:04:22 INFO SLOT 4 GAME Event Code: 9
BackBone 3 became re-connected
11: 05/08/95 16:04:22 DEBUG SLOT 4 GAME Event Code: 73
#REMOTE 2 FSM: DOWN -> SYNC (000011: a0000007 000041 10000000 10000000)

Figure 3-2. Events Manager Window

You can scroll through the event messages using the scroll bars on the bottom and right side of the window. Select Ascending to display events from the oldest to the most recent. Select Descending to display events from the newest (most recent) to the oldest.

Displaying a Remote Log

A remote log resides on the router's memory card or diskette. To display the log, you must retrieve it from the router's media. Connect to the router whose event messages you want to view. Then, proceed as follows:

1. **From the Events Manager window, select File→Get Remote Log File.**

   The Load Remote Log File window appears (Figure 3-3).

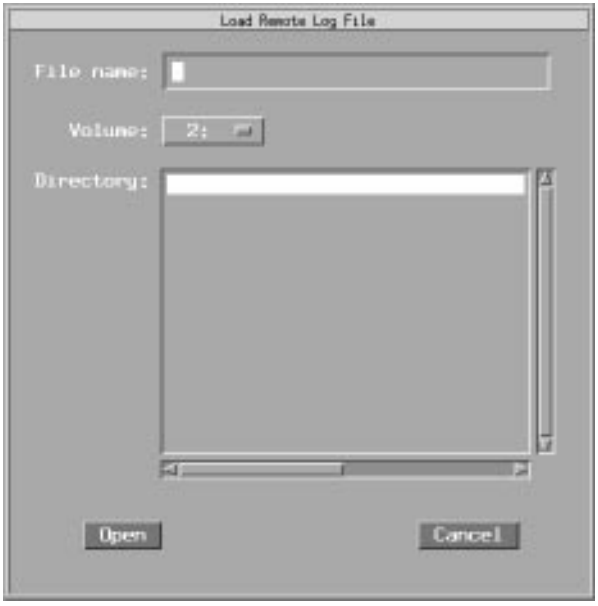

Figure 3-3. Load Remote Log File Window

2. **Select the volume that contains the log file from the Volume pull-down menu.**
3. **Enter the filename.**
4. **Click on Open.**

The router transfers the file to the Site Manager workstation, where Site Manager displays the events listed in the file in the Events Manager window. Along with event messages from the router's memory card or diskette, the following data appears in the Events Manager window:

- The filename you selected, in the Log Filename field
- `Remote Log`, in the Log File Source field
- The total number of events, in the Number of Records field

Displaying a Local Log

A local log resides on the hard drive of your Site Manager workstation. Before you can display any event messages, you must connect to the router whose event log you want to view. After doing this, proceed as follows:

1. **From the Events Manager window, select File→Load Local Log File.**

   The Load Local Log window appears (Figure 3-4).

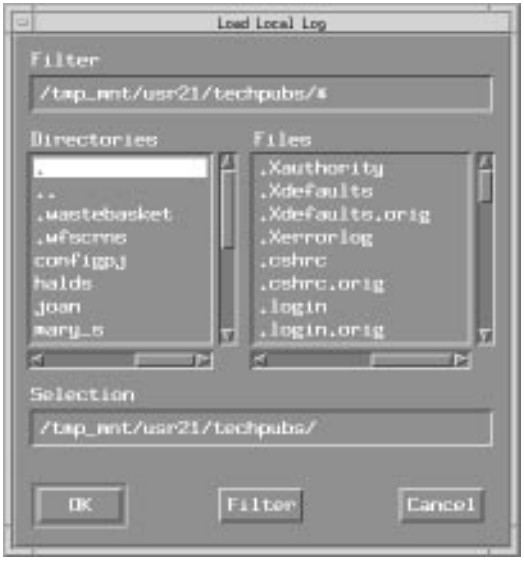

Figure 3-4. Load Local Log Window

2. **Select the directory that contains the log file in the Directories box until the path to the directory appears in the Selection window.**

3. **Select or type in the filename in the Selection box after the pathname.**
4. **Click on OK.**

Along with the event messages from this file, the Events Manager window displays

- The filename you selected, in the Log Filename field
- The name `Local Log`, in the Log File Source field
- Total events, in the Number of Records field

Filtering Event Messages

You can specify the types of event messages that appear in the Events Manager window by specifying *filters*. You can filter event messages by severity, slot, entity, or router IP address. The Filters feature in the Trap Monitor window specifically filters for severity, slot, and entity.

Note: *Filtering does not affect how events are logged in the router's memory. Event messages are filtered only in the Events Manager window, not in their source.*

Filtering by Severity, Slot, and Entity

You can filter event messages displayed in the Events Manager window as follows:

1. **Display events in the Events Manager window.**
2. **Select View→Filters.**

   The Filtering Parameters window appears (Figure 3-5).

   This window highlights the activated parameters. You can click on Toggle to switch between highlighted and nonhighlighted options.

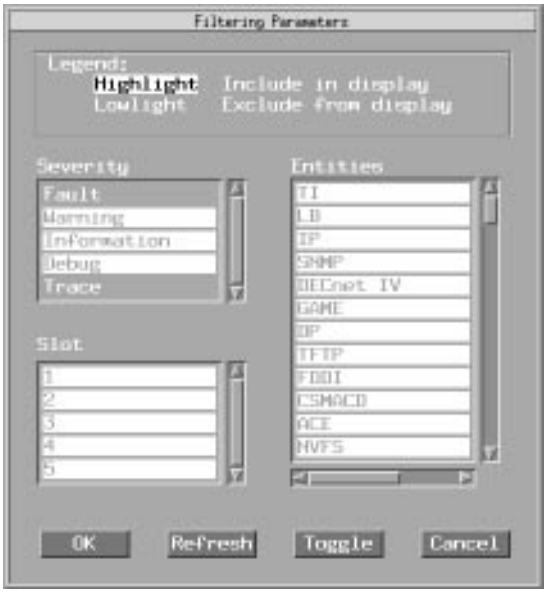

Figure 3-5. Filtering Parameters Window

You can change the current filtering setup by highlighting any Severity, Slot, or Entities parameter you want included in the next event log display. You can then do the following:

— Click on Refresh to refilter the event messages.

— Click on OK to save your new filtering setup without automatically refiltering the event messages.

3. **Select the parameters you want, and then click on Refresh or OK.**

Notice that the number of records does not change; the total number of event messages is always displayed.

Note: *We recommend filtering for trace events only when you diagnose network problems. You do not need to filter for debug events.*

Filtering by Router IP Address

Filtering by router IP address requires that you connect to a router from the main Site Manager window or Events Manager window. See the earlier section "Connecting to a Router." Then display a current, remote, or local event log using the File menu. See "Displaying Event Logs," described earlier.

Event messages now appear in the Events Manager window. You have effectively "filtered" a log by router IP address.

Searching for an Event Message

Use the Events Manager's Find and Find Next options to locate an event containing text that you specify:

1. **Display events in the Events Manager window.**
2. **Select Find→Find.**

   The Find Text Pattern window appears (Figure 3-6).

Figure 3-6. Find Text Pattern Window

3. **Type the text you want to find.**

   You can type up to 255 characters (including spaces) in this box.

Note: *The Find Text Pattern window is case-sensitive.*

4. **Click on Find.**

   Site Manager searches from the first event highlighted in the log for the first instance of the text pattern and highlights the event that contains the text pattern.

5. **Select Find→Find Next to find the next instance of the same text pattern.**

Refreshing the Events Manager Window

To redisplay a log file in Site Manager's memory after you set up new filters, select View→Refresh Display, from the Events Manager window.

The Events Manager displays the events that match the filters you last saved, according to the setting of the Ascending/Descending option in the Events Manager window.

Clearing the Events Manager Window

To clear the events in the Events Manager window, select View→Clear Window. The window clears and remains empty until you load an event log or refresh the display.

Saving Event Messages

You can save the event messages that appear in the Events Manager window to an ASCII file on your Site Manager workstation. You can then print the log, using any tool on your workstation.

To save an event log to an ASCII file, follow these steps:

1. **Display the event log in the Events Manager window.**
2. **Filter the event messages displayed.**
3. **Select File→Save Output to Disk.**

   The Save Log window appears (Figure 3-7).

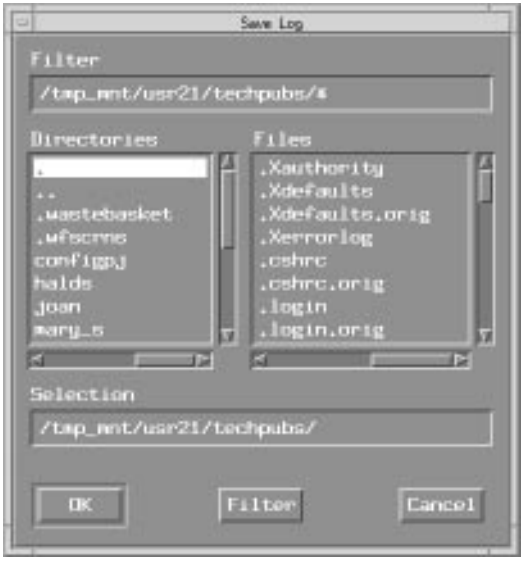

Figure 3-7. Save Log Window

4. **Select the directory path in which you want to save the file.**

   The path appears in the Selection window.

5. **Enter the filename in the Selection window after the path.**

6. **Click on OK.**

   The Events Manager saves the log to an ASCII file in the specified local directory. (If you do not specify a directory, the file is automatically saved to your local directory.)

Note: *For viewing purposes, you can reload into the Events Manager event logs stored in binary format. You cannot reload into the Events Manager event logs stored in ASCII format.*

Clearing the Current Event Log

The router's event log can hold only a fixed number of messages. When it reaches its limit, it starts overwriting the log at the beginning. To clear a router's current event log, select Administration→Clear Event Log, from the main Site Manager window. A confirmation window appears (Figure 3-8).

Figure 3-8. Confirmation Window

Click on OK in the confirmation window to delete all the event messages that are currently stored in the router's memory. Site Manager enters a message in the event log indicating that it has cleared the log. New event messages automatically start filling the event log again.

Chapter 4
Monitoring Statistics

For general information about monitoring router statistics, see “Monitoring Statistics” in Chapter 1. For specific information about using buttons, windows, and other Site Manager features, refer to *Using Site Manager Software*. For information on file-based performance statistics, refer to *Gathering and Interpreting Performance Data (BNX Software)*.

You can use Site Manager to do the following:

- Access statistics
- Connect to a router
- View the Bay Networks MIB
- Define the current screen list
- Display statistics screens
- Create statistics filters
- Search for statistics information
- Save statistics information
- Build custom statistics screens
- Use the MIB II Counters feature

Accessing Statistics

You access all router statistics from the Statistics Manager window. To access this window, begin at the main Site Manager window and click on Statistics, or select Tools➔Statistics Manager. The Statistics Manager window appears (Figure 4-1).

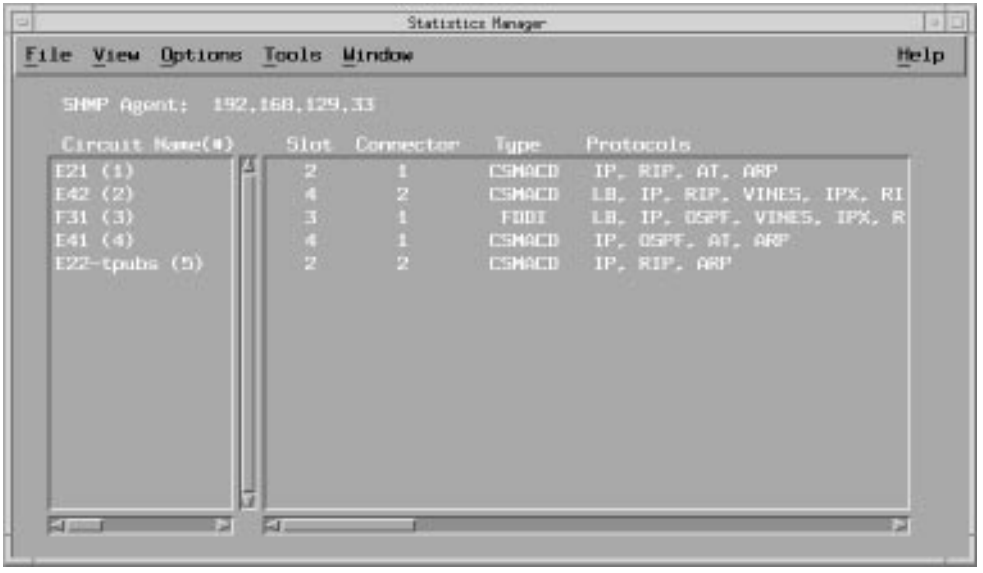
Statistics Manager
File View Options Tools Window Help
SNMP Agent: 192.168.129.33
Circuit Name(#) Slot Connector Type Protocols
E21 (1) 2 1 CSMACD IP, RIP, AT, ARP
E42 (2) 4 2 CSMACD LB, IP, RIP, VINES, IPX, RI
F31 (3) 3 1 FDDI LB, IP, OSPF, VINES, IPX, R
E41 (4) 4 1 CSMACD IP, OSPF, AT, ARP
E22-tpubs (5) 2 2 CSMACD IP, RIP, ARP

Figure 4-1. Statistics Manager Window

Note: *The Statistics Manager requires an active connection to a target router to display router statistics. The next section describes how to use the Statistics Manager tool to establish or change a connection to a router.*

The Statistics Manager window displays the current router's configuration. That is, it displays the circuit type and location of the router's network interfaces and the bridging and routing protocols that are enabled on each interface.

Connecting to a Router

To connect to a router from the Statistics Manager window, proceed as follows:

1. **Select Options→Router Connection.**

   The Router Connection Options window appears (Figure 4-2).

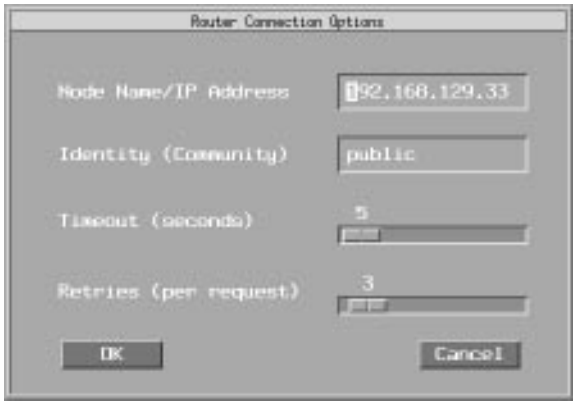

Figure 4-2. Router Connection Options Window

2. **Specify the target router's IP address in the Node Name/IP Address field. Then click on OK.**

The SNMP Agent field in the Statistics Manager window displays the IP address of the router you specified. (See Figure 4-1.)

Viewing the Bay Networks MIB

You view the Bay Networks Management Information Base (MIB) using the Quick Get tool. Quick Get includes a MIB Browser tool that lets you scroll through and select up to ten objects from the MIB. You then use Quick Get to get all instances of objects you select and to display that information in columns in the Quick Get Facility window.

To access the Quick Get Facility window, begin at the Statistics Manager window and select Tools→Quick Get. The Quick Get Facility window appears (Figure 4-3).

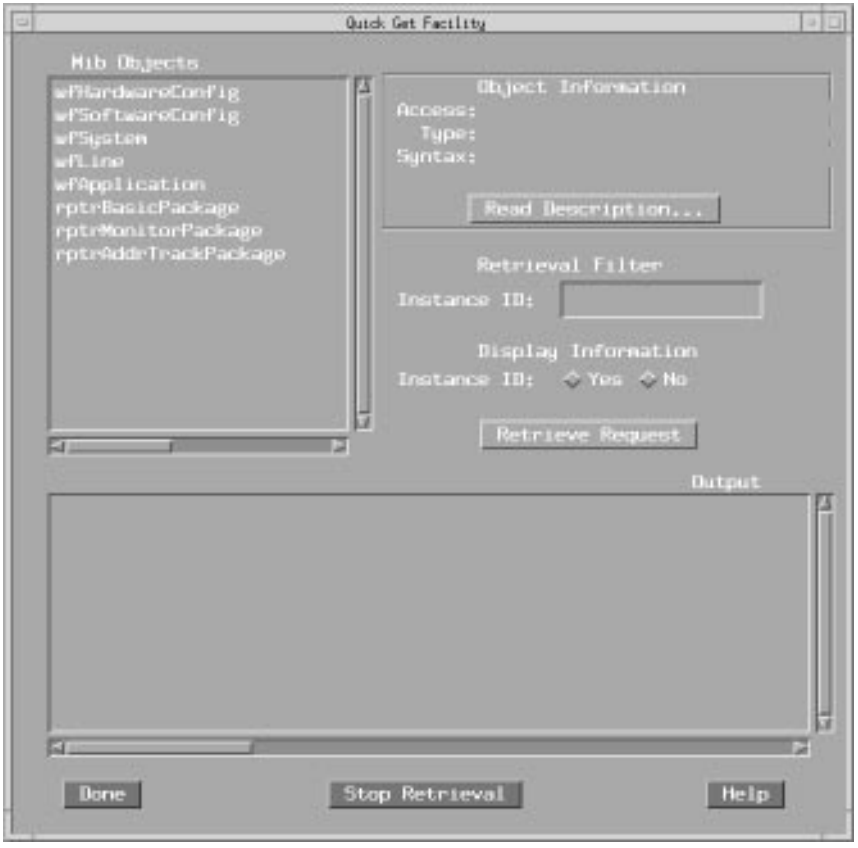

Figure 4-3. Quick Get Facility Window

The MIB Browser operates the MIB Objects window located in the top-left corner of the window.

Using the MIB Browser

The Bay Networks MIB is organized as a hierarchical tree. When you first activate Quick Get, the MIB Browser displays the object groups at the top of the tree:

- wfHardwareConfig
- wfSoftwareConfig
- wfSystem
- wfLine
- wfApplication
- rptrBasicPackage
- rptrMonitorPackage
- rptrAddrTrackPackage

Beneath these object groups, related objects are organized in subordinate object groups, or tables (for example, Figure 4-4 shows part of the MIB tree for the wfSystem object group). The prefix wf that precedes many of the MIB objects indicates that they are Bay Networks enterprise-specific objects.

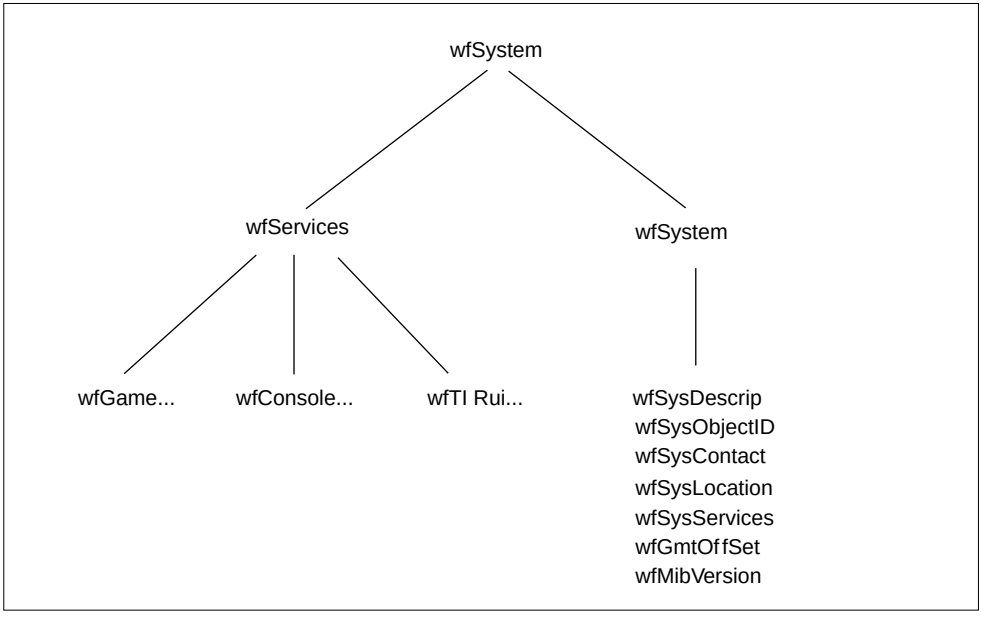

Figure 4-4. MIB Tree for System Group

To access individual objects, first select the top-level object group. The MIB Browser brings you down one level in the tree and displays subordinate object groups. Continue selecting object groups and descending through the MIB tree until the MIB Browser displays the individual objects that you want to select.

You can differentiate between object groups and individual objects by noting their position in the MIB Browser window. Object groups are flush left with the window; individual objects are indented slightly.

Use the scroll bar to scroll through the MIB. To move backward in the MIB tree, select the Back option, which appears in the Quick Get Facility window after you display subordinate object groups from the top-level object group.

Table 4-1 describes where to find different types of MIB information.

Table 4-1. Finding MIB Information

Top-level MIB Object Group	Types of Objects/Information	Example
wfHardwareConfig	Objects pertaining to router hardware configuration	Router backplane ID, power supply, temperature, serial number
wfSoftwareConfig	Objects pertaining to the type of protocol and driver software that is loaded, and information required to load the software	Interface drivers
wfSystem	Objects pertaining to the router system software	System record, console, remote console, circuit name table
wfLine	Objects pertaining to drivers and lines	FDDI tables, line state, line traffic
wfApplication	LAN, WAN, and Bridge information	Routing tables, packet information, protocol state information
rptrBasicPackage	Repeater configuration, status, and control information	Repeater operational state
rptrMonitorPackage	Objects that monitor repeater performance statistics	Performance and error statistics for groups and ports
rptrAddrTrackPackage	Table of address mapping information about the repeater ports	Source address of the last readable frame that the port received

Getting Instances of Selected Objects

You can select and retrieve instances for as many as ten MIB objects at one time. To locate individual objects, find the object group or table that logically categorizes the objects you are interested in.

Proceed as follows:

1. **Select the top-level object group to which the objects belong.**

   The MIB Objects field displays a list of subordinate groups. For example, when you select wfApplication, the objects shown in Figure 4-5 appear.

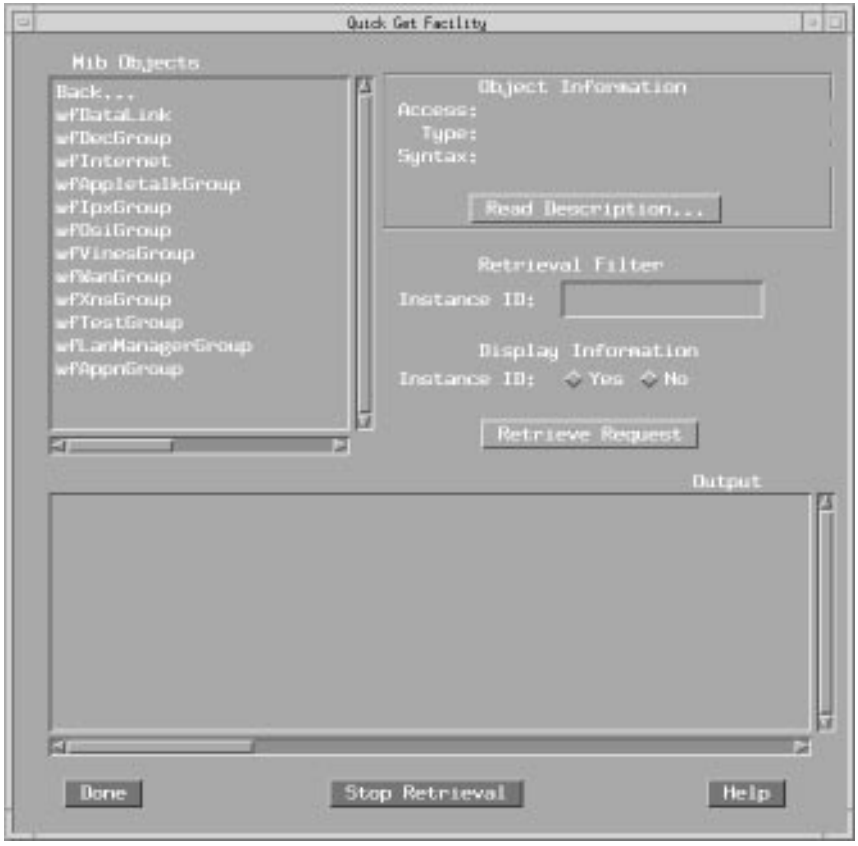

Figure 4-5. Sample Quick Get Facility Window

2. **Select additional object groups or tables until you reach the individual objects you are interested in.**

   For example, to see the current state of all IP interfaces configured on the router, select wfInternet, wfIpRouting, wfIpGroup, wfIpInterfaceTable. Then select the wfIPInterfaceState and wfIPInterfaceAddr objects located beneath the wfIpInterfaceTable group.

3. **Select each object in which you are interested. Note that selectable objects are indented.**

   When you select an individual object, the Object Information field at the top right of the Quick Get Facility window displays the following information about that object:

Access	Whether the object is user configurable (read-write) or nonconfigurable (read-only)
Type	The type of object (integer, octet, string)
Syntax	The possible values for the object

   Click on Read Description to display a Statistics Help window that contains a more detailed description of the object. Click on OK to exit the Statistics Help window.

   To deselect an object listed under MIB Objects, select the object again.

4. **Use selections in the Display Information and Retrieval Filter fields of the Quick Get Facility window to determine the format of MIB objects retrieved to the Output field of that window.**

   You can use the Quick Get Facility to display

   — All (unfiltered) or specific (filtered) instances of MIB objects selected in the Mib Objects field

   — All (filtered or unfiltered) instances of selected MIB objects, with or without their associated instance IDs

To display without instance IDs all instances of MIB objects selected in the Mib Objects field (Figure 4-6):

a. **Leave the Retrieval Filter field blank.**

b. **Select No in the Display Information field.**

c. **Click on Retrieve Request.**

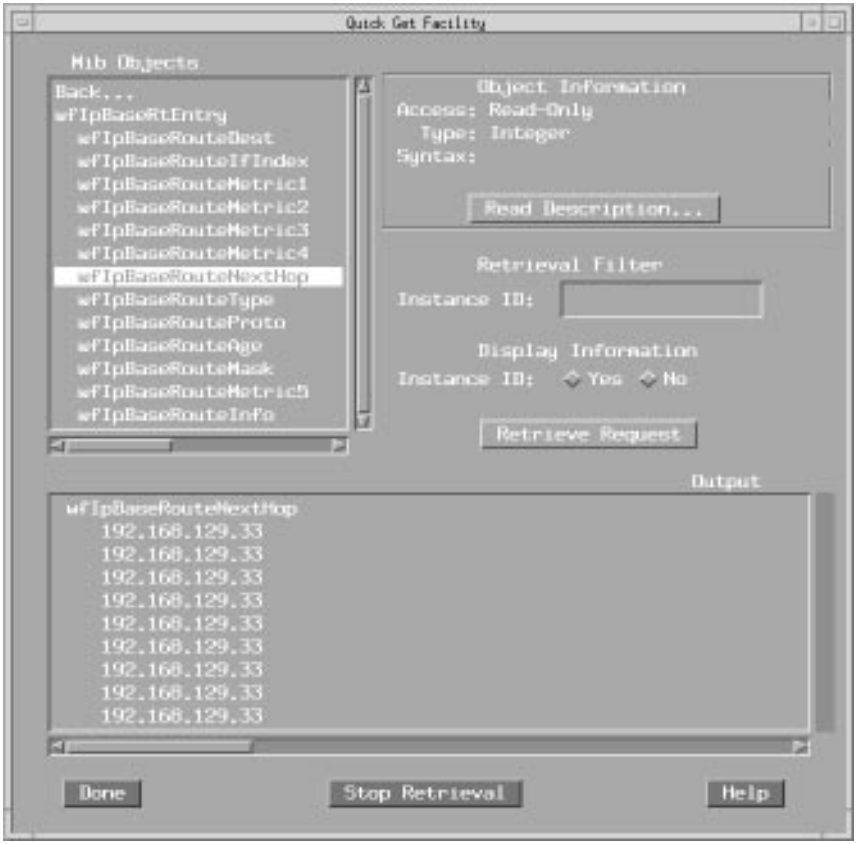

Figure 4-6. All Instances Retrieved (Unfiltered) without Instance IDs

To display with instance IDs all instances of MIB objects selected in the Mib Objects field (Figure 4-7):

a. **Leave the Retrieval Filter field blank.**

b. **Select Yes in the Display Information field.**

c. **Click on Retrieve Request.**

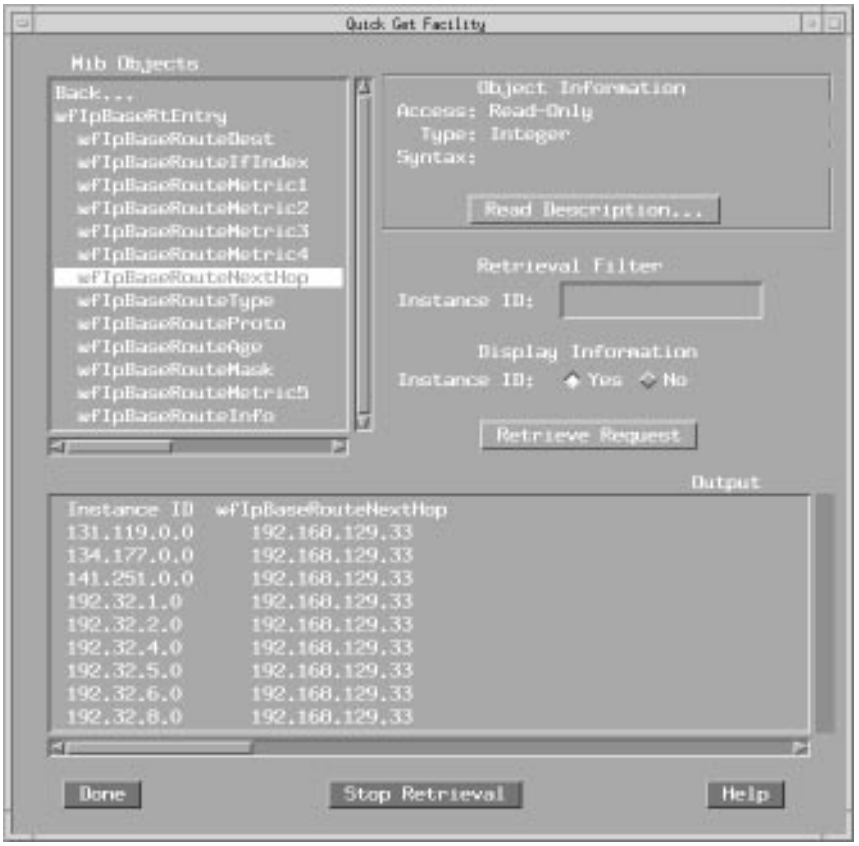

Figure 4-7. All Instances Retrieved (Unfiltered) with Instance IDs

To display without instance IDs only specific (filtered) instances of MIB objects selected in the Mib Objects field (Figure 4-8):

a. **Enter all or part of the instance ID for the desired MIB object(s) in the Retrieval Filter field.**

   Entering more of the instance ID narrows the object search.

b. **Select No in the Display Information field.**

c. **Click on Retrieve Request.**

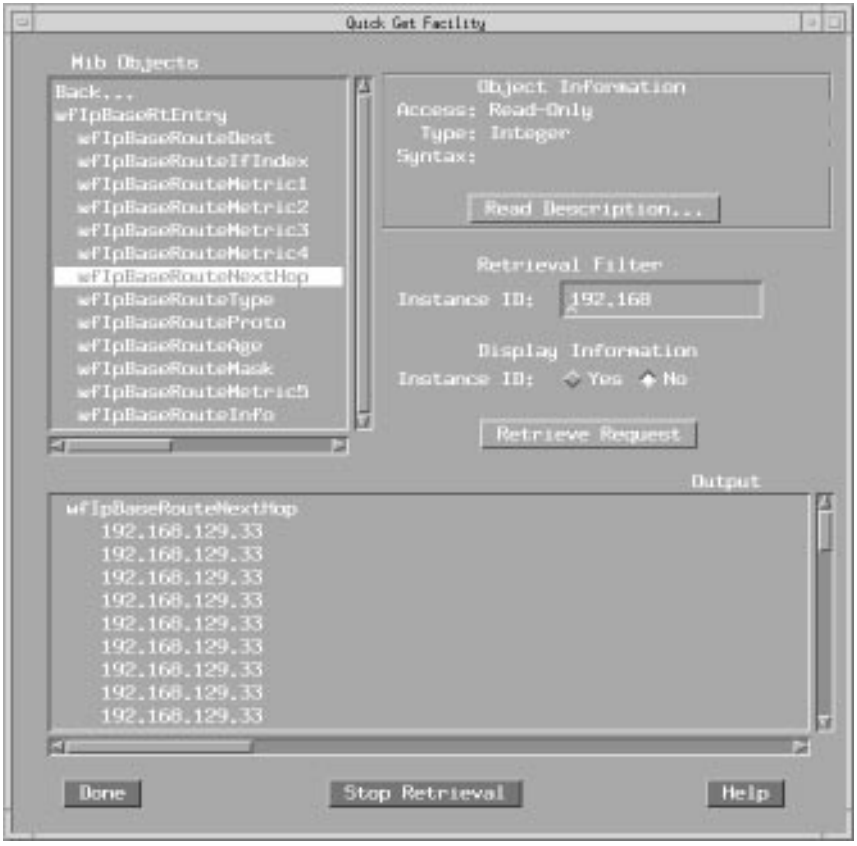

Figure 4-8. Specific Instances Retrieved without Instance IDs

To display with instance IDs only specific (filtered) instances of MIB objects selected in the Mib Objects field (Figure 4-9):

a. **Enter all or part of the instance ID for the desired MIB object(s) in the Retrieval Filter field.**

   Entering more of the instance ID narrows the object search.

b. **Select Yes in the Display Information field.**

c. **Click on Retrieve Request.**

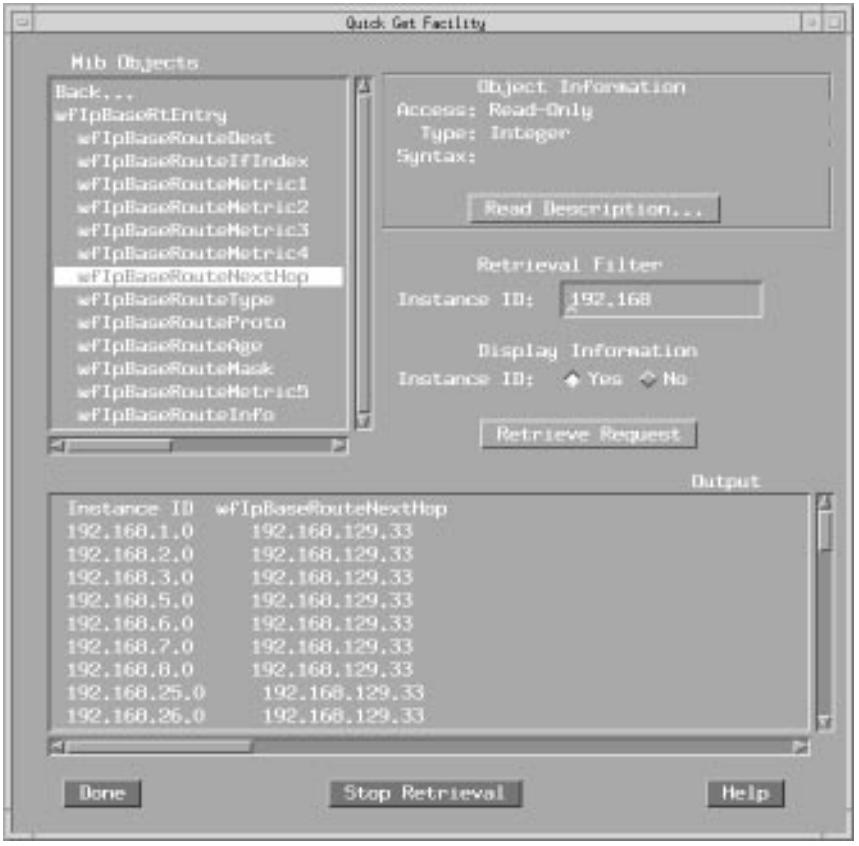

Figure 4-9. Specific Instances Retrieved with Instance IDs

5. **Click on Stop Retrieval to halt retrieval of objects selected in the Mib Objects field.**

6. **Click on Retrieve Request each time you want to refresh the information displayed in the Output field.**
7. **To exit the Quick Get Facility window, click on Done.**

Defining the Current Screen List

The current screen list is a subset of the default statistics screens and any custom statistics screens you build. (More information follows on the Screen Builder tool you use to custom design router statistics screens.)

Note: *When you first use the Statistics Manager, the current screen list is empty. To view router statistics, you must add statistics screens to the current screen list.*

To manage your statistics screen database most effectively, add to the current screen list only those statistics screens that you use most often.

Adding Statistics Screens

To add a statistics screen to the current screen list, follow these steps:

1. **From the Statistics Manager window, select Tools→Screen Manager.**

   The Screen Manager window appears (Figure 4-10).

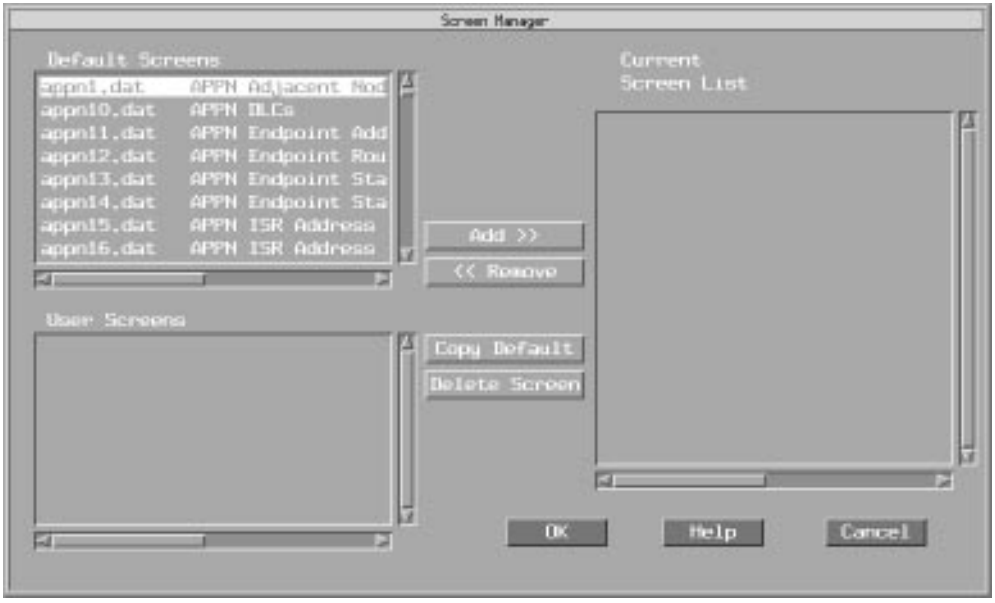

Figure 4-10. Screen Manager Window

The Screen Manager displays the default statistics screens, grouped by protocol. Use the scroll bar to scroll through the list. If you have not yet built any custom statistics screens, then the User Screens list is empty. Later, it will display any custom screens you create using the Screen Builder.

The Statistics Manager identifies each default statistics screen using a filename with the *.dat* extension, followed by a description of the type of data the screen displays. In the example shown in Figure 4-11, the statistics screen displays IP routing statistics.

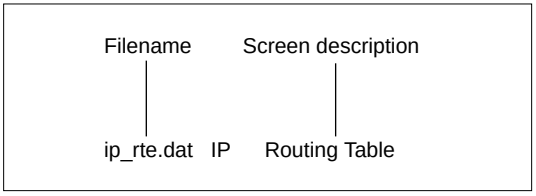

Figure 4-11. Example of Filename and Screen Description

2. **Highlight the statistics screen you want to add to the Current Screen List, then click on Add.**

   The Current Screen List can contain both default screens and custom screens at the same time, so you can add statistics screens from either list. The Statistics Manager updates the Current Screen List to include the statistics screen that you add.

   Repeat Steps 1 and 2 to add additional statistics screens to the current screen list.

3. **Click on OK to update the current screen list and save your changes, or click on Cancel to exit the Screen Manager window without saving the changes.**

You can use the Launch Facility to display any screen on the current screen list. For instructions, see "Displaying Statistics Screens" later in this chapter.

Removing Statistics Screens

To remove a statistics screen from the Current Screen List, follow these steps:

1. **From the Statistics Manager window, select Tools→Screen Manager.**

   The Screen Manager window appears.

2. **Highlight the statistics screen you want to remove from the current screen list. Then click on Remove.**

   The Statistics Manager removes the statistics screen you select. Repeat Steps 1 and 2 to remove additional statistics screens.

3. **Click on OK to exit the window and save your changes, or click on Cancel to exit without saving the changes.**

Displaying Statistics Screens

Use the Launch Facility to display statistics screens.

Note: *Before you can display a statistics screen, you must add it to the current screen list. For instructions, see the previous section, "Defining the Current Screen List."*

To display a statistics screen, follow these steps:

1. **From the Statistics Manager window, select Tools→Launch Facility.**

   The Statistics Launch Facility window displays the statistics screens that are in the Current Screen List (Figure 4-12).

Figure 4-12. Statistics Launch Facility Window

2. **Select one of the statistics screens and click on Launch.**

Once you launch the statistics screen, Site Manager begins retrieving the specified MIB objects from the router. After a short time, a statistics screen appears, such as the one shown in Figure 4-13.

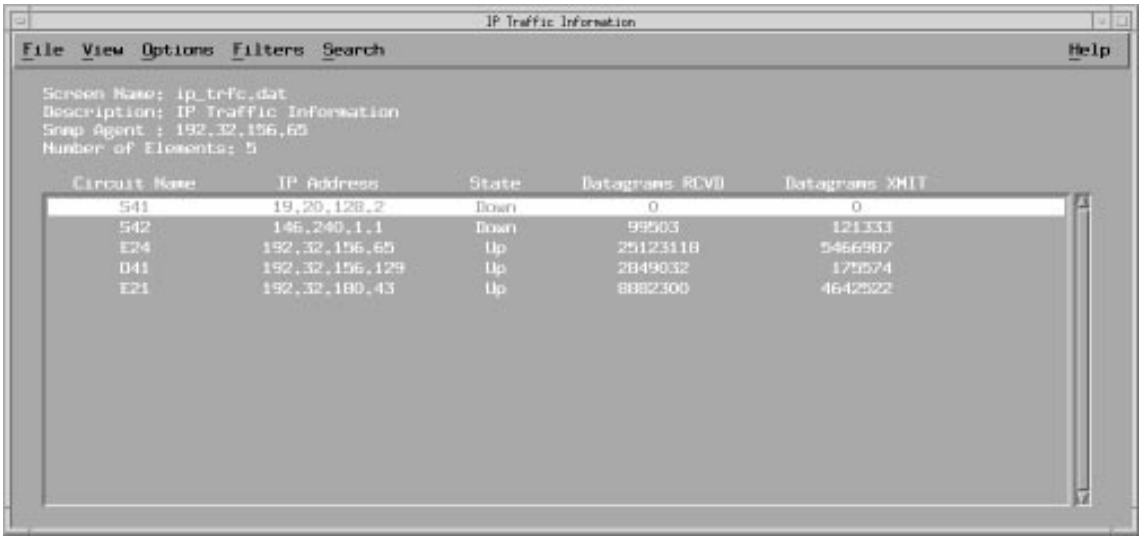
IP Traffic Information
File View Options Filters Search Help
Screen Name: ip_trfc.dat
Description: IP Traffic Information
Snmp Agent : 192.32.156.65
Number of Elements: 5
Circuit Name IP Address State Datagrams RCVD Datagrams XMIT
S41 19.20.128.2 Down 0 0
S42 146.240.1.1 Down 99503 121333
E24 192.32.156.65 Up 25123118 5466987
D41 192.32.156.129 Up 2849032 175574
E21 192.32.180.43 Up 8882300 4642522

Figure 4-13. Statistics Screen

Refreshing Active Statistics Screens

To update a statistics screen, select View→Refresh Display.

The Statistics Manager retrieves the MIB objects from the router and updates the statistics screen with the new data.

Specifying Circuit Mode Statistics Polling Rate

A circuit mode statistics screen is one that the Statistics Manager continually updates with new data. When viewing a circuit mode screen, you can specify how often the Statistics Manager polls the router to update the data.

To specify the polling rate, begin at a statistics screen and proceed as follows:

1. **Select Options→Poll Rate.**

   The Polling Rate window appears (Figure 4-14).

Figure 4-14. Polling Rate Window

2. **Use the slidebar to specify a polling rate; then click on OK.**

Zeroing Circuit Mode Statistics

You can reset all counters in a circuit mode statistics screen to zero through the Zero All Counters menu option. You can also reset all counters in a selected row to zero through the Zero Current Row Counters menu option.

Note: *These functions affect only the values displayed in Site Manager circuit mode statistics windows, and have no effect on the actual value of counter objects in a router MIB.*

Zeroing All Counters in a Screen

To clear all counters in a circuit mode statistics screen, select Options→Zero All Counters.

Figure 4-15 shows a typical response to the Zero All Counters option.

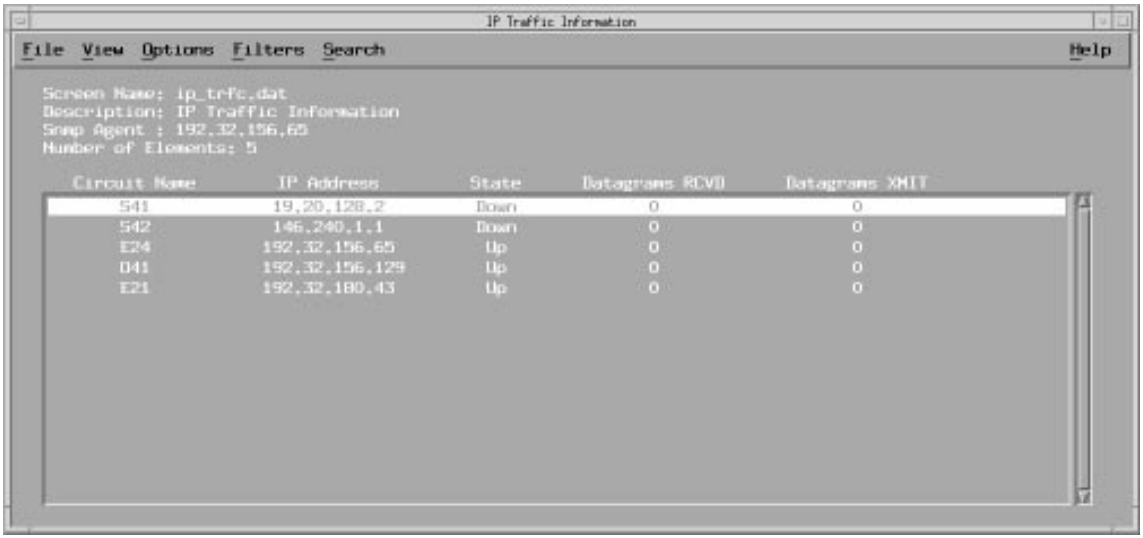

Figure 4-15. Zeroing All Counters in a Screen

Note: *In this example, the counters Datagrams RCVD and Datagrams XMIT reset to zero in the statistics screen. This type of reset has no effect on the actual, current values of these counter objects in the router MIB.*

The Zero All Counters command stores the value of every counter object in the display at reset time. Each stored value provides a reference point for counter values displayed following the reset; that is, after resetting all counters in the display.

- The Statistics Manager displays only the difference between the counter value at reset time (the last known reference value) and the actual, current (MIB) value of the same counter.
- The counter values in display reflect *the amount of change* incurred beyond the reference values stored at reset time.

Zeroing All Counters in a Specific Row

To clear all counters in a specific row of a circuit mode statistics screen, select a row, then select Options➔Zero Current Row Counters.

Figure 4-16 shows a typical response to the Zero Current Row Counters option.

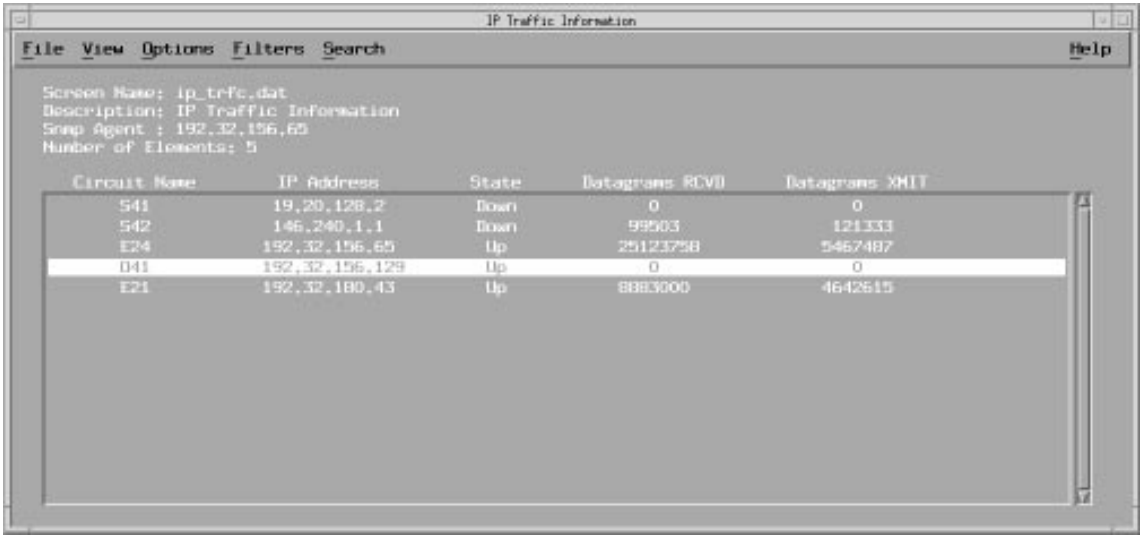
IP Traffic Information
File View Options Filters Search Help
Screen Name: ip_trfc.dat
Description: IP Traffic Information
Snmp Agent : 192.32.156.65
Number of Elements: 5
Circuit Name IP Address State Datagrams RCVD Datagrams XMIT
S41 19.20.128.2 Down 0 0
S42 146.240.1.1 Down 99503 121333
E24 192.32.156.65 Up 25123758 5467487
D41 192.32.156.129 Up 0 0
E21 192.32.180.43 Up 8883000 4642615

Figure 4-16. Zeroing All Counters in a Specific Row

The counters Datagrams RCVD and Datagrams XMIT reset to zero in the selected row. The reset has no effect on the actual, current values of these counter objects in the router MIB.

The Zero Current Row Counters command stores the value of every counter object displayed in the selected row at reset time. Each stored value provides a reference point for counter values displayed in the selected row after you zero the current row counters.

- The Statistics Manager displays only the difference between the counter value at reset time (the last known reference value) and the actual, current (MIB) value of the same counter.
- The counter values in display reflect *the amount of change* incurred beyond the reference values stored at reset time.

Stopping Statistics Retrieval

To stop the Statistics Manager from collecting any further statistics in the current screen, select View➔Stop Retrieval.

Creating Statistics Filters

You can set a *display filter* or a *retrieval filter* for each statistics screen you open from the Statistics Manager Launch Facility.

Without filtering, the Statistics Manager polls a router for the values of all MIB objects defined in the currently active statistics screen. The screen subsequently shows the values of those objects, as determined by the data returned by the router.

A *display filter* is a software mechanism that enables the Statistics Manager to search the entire contents of the currently active statistics screen and then

- *Show* only those rows that contain an object that contains a string matching in value to the filter string. (This is the display filter's Display option.)
- *Hide* only those rows that contain an object that contains a string matching in value to the filter string. (This is the display filter's No Display option.)

Specifying a longer display filter string narrows the number of match possibilities available from the currently active statistics screen.

A *retrieval filter* is a software mechanism that enables the Statistics Manager to poll a router for only a subset of specific MIB objects. These objects have instance IDs that match the full or partial instance ID you enter in the Retrieval Filter window.

The currently active statistics screen subsequently displays the values of those objects, as determined by the data returned by the polled router. The Statistics Manager polls only one router in each statistics window.

The retrieval filtering mechanism for a statistics screen works substantially in the same way as does the retrieval filtering mechanism for the Quick Get Facility. That is, specifying more of the instance ID in the Retrieval Filter window causes the workstation to solicit a smaller number of objects from a router. This, in turn, typically reduces the number of objects displayed in the active statistics screen.

Using retrieval filters to collect statistics across your network reduces

- The amount of processing overhead performed by your Site Manager workstation and any polled router
- The amount of network bandwidth consumed for the purpose of periodic polling and poll responses

You can use display filters and retrieval filters in various combinations. For example, you could

- Use a retrieval filter first to solicit from routers in your network the values of certain MIB objects
- Apply a display filter to hide or show objects in the resulting statistics screen

Using Display Filters

To create a display filter, begin from a statistics screen:

1. **Select Filters→Display Filters.**

   The Display Filters window prompts you to define the filter (Figure 4-17).

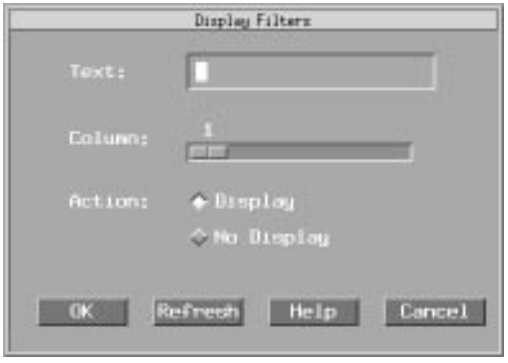

Figure 4-17. Display Filters Window

2. **Enter the text string you want to filter in the Text field.**
3. **Specify the column where you want the filter to take effect.**

   Use the slidebar to select the column that displays the statistics that you want to filter.

   In this case, Site Manager displays the statistics for the address mask in Column 5. Thus, you use the slidebar to specify Column 5.

4. **Select either Display or No Display, depending on the desired action.**

   If you want the Statistics Manager to display only those statistics that match the filter, select Display. If you want the Statistics Manager to hide those statistics that match the filter, select No Display.

5. **Click on OK to save the filter in memory, or click on Refresh to implement the filter immediately.**

   — If you click on OK, the filter box disappears. There will be no immediate change to the statistics screen. However, the next time you refresh the statistics screen, it will display only the statistics specified by the filter.

   — If you click on Refresh, the Statistics Manager immediately refreshes the screen and displays only the statistics specified by the filter.

6. **Click on OK to exit the Display Filters window.**

Display Filter Example:

In Figure 4-18, if you want to display the statistics only for the circuit with an IP address of 192.32.180.43, configure the display filter shown in Figure 4-19.

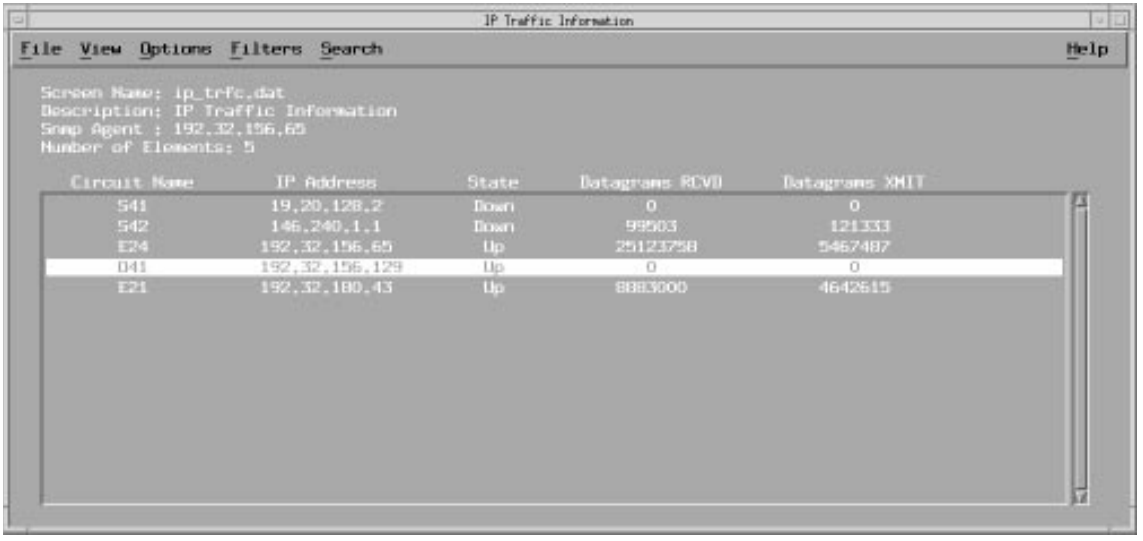
IP Traffic Information
File View Options Filters Search Help
Screen Name: ip_trfc.dat
Description: IP Traffic Information
Snmp Agent : 192.32.156.65
Number of Elements: 5
Circuit Name IP Address State Datagrams RCVD Datagrams XMIT
S41 19.20.128.2 Down 0 0
S42 146.240.1.1 Down 99503 121333
E24 192.32.156.65 Up 25123758 5467487
D41 192.32.156.129 Up 0 0
E21 192.32.180.43 Up 8883000 4642615

Figure 4-18. Statistics Window Unfiltered

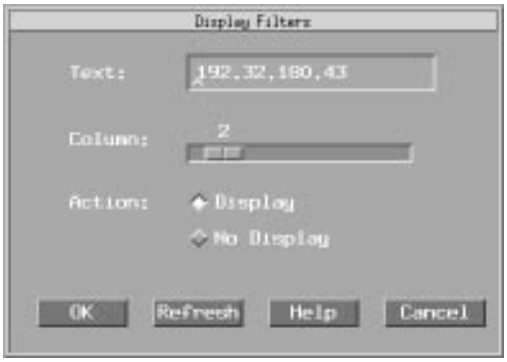

Figure 4-19. Sample Display Filters Window

When you click on Refresh in the Display Filters window (Figure 4-19), the Statistics Manager filters out of the active statistics window the line with the IP address of 192.32.180.43 in Column 2.

Figure 4-20 shows the result of applying the display filter to the active statistics window.

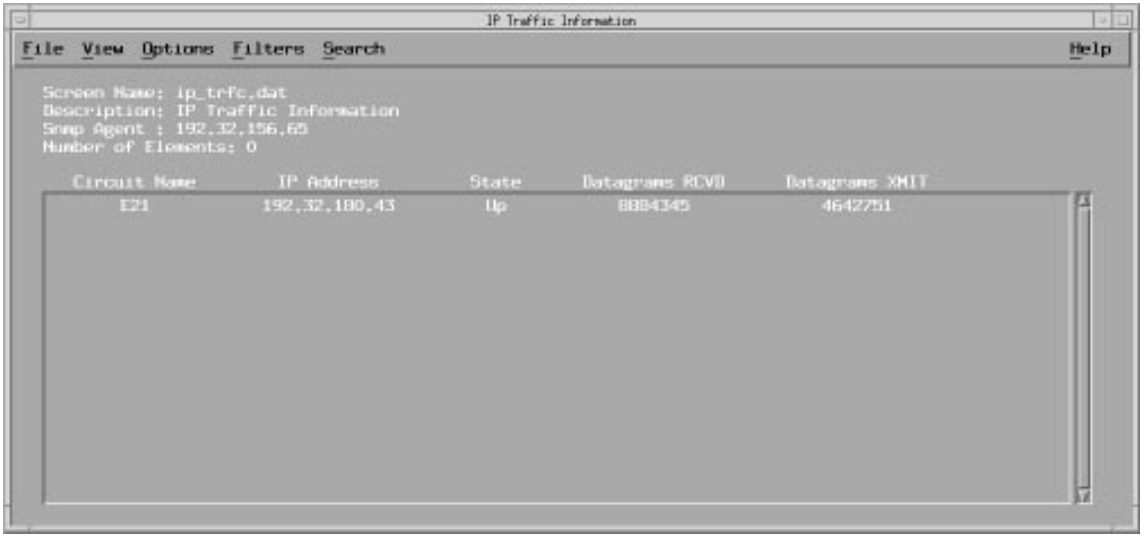

Figure 4-20. Statistics Screen after Filter Implemented

Using Retrieval Filters

To create a retrieval filter, begin from a statistics screen:

1. **Select Filters→Retrieval Filters.**

   The Retrieval Filters window appears (Figure 4-21).

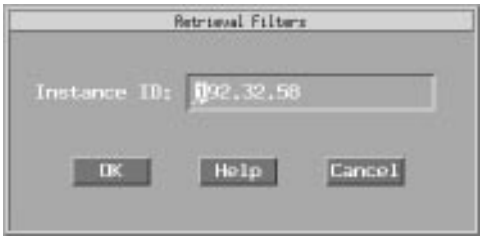

Figure 4-21. Retrieval Filters Window

2. **Enter the instance ID of the object(s) you want to view.**

   Specifying a partial ID causes the Statistics Manager to poll and display all objects that begin with the same partial ID.

3. **Click on OK to save the filter in memory associated with the current statistics screen.**

4. **Select View→Refresh Display, from the statistics screen.**

Figure 4-22 shows the result of this retrieval filter. The Statistics Manager retrieves only one MIB object; no other instances of the same object exist in the MIB associated with the currently connected router.

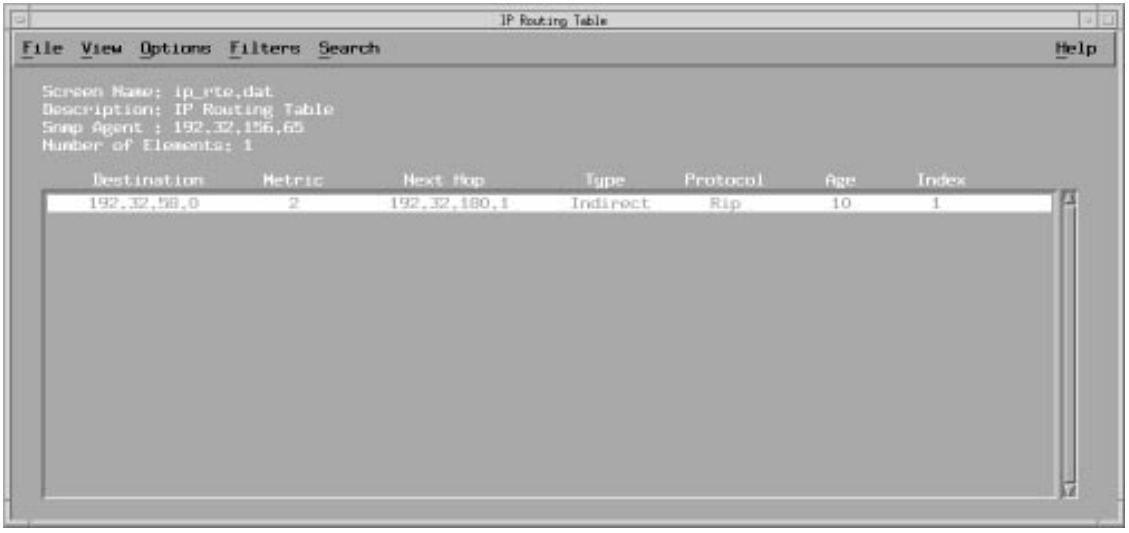
IP Routing Table
File View Options Filters Search Help
Screen Name: ip_rte.dat
Description: IP Routing Table
Snmp Agent : 192.32.156.65
Number of Elements: 1
Destination Metric Next Hop Type Protocol Age Index
192.32.50.0 2 192.32.180.1 Indirect Rip 10 1

Figure 4-22. Statistics Screen after Implementing a Retrieval Filter

Searching for Statistics Information

You can search for any text string that appears on a statistics screen.

To define the text string to search for, proceed as follows:

1. **Select Search→Find.**

   The Statistics Manager displays a Search Options window that prompts you to define a text string (Figure 4-23).

Figure 4-23. Search Options Window

2. **Enter the text you want to search for; then click on Find.**

The Statistics Manager highlights the line where the next instance of the text string occurs. Continue clicking on Find in the Search Options window.

Note: *The Search Options window is case-sensitive.*

If you still want to search for the text string you defined, but would rather have the Search Options window disappear, proceed as follows:

1. **Click on Cancel in the Search Options window.**

   The Search Options window disappears.

2. **Select Search→Find Next.**

   The Statistics Manager highlights the line where the next instance of the text string occurs.

Saving Statistics Information

The Statistics Manager allows you to save the information displayed on a statistics screen to an ASCII file on your Site Manager workstation.

To save the information shown on the statistics screen, proceed as follows:

1. **Select File→Save As from the statistics screen.**

   A file directory box appears, prompting you to select a place to store the data.

2. **Select a directory in which to store the data.**

3. **Select a file in which to store the data.**

   You can select an existing file from the file list or type a new name for the file in the Filename field.

4. **Click on OK.**

   Site Manager stores the data in ASCII format.

You can use any text editor to view the data once you store it on your workstation.

Building Custom Statistics Screens

You can build custom statistics screens. You can select up to nine different objects from the Bay Networks MIB and define how the screen displays the statistics you select. After you save the custom statistics screen, it is added to the Screen Manager's user screen list.

Designing Statistics Screens

To design a custom statistics screen, proceed from the Statistics Manager window as follows:

1. **Select Tools→Screen Builder.**

   The Screen Builder Facility window appears (Figure 4-24).

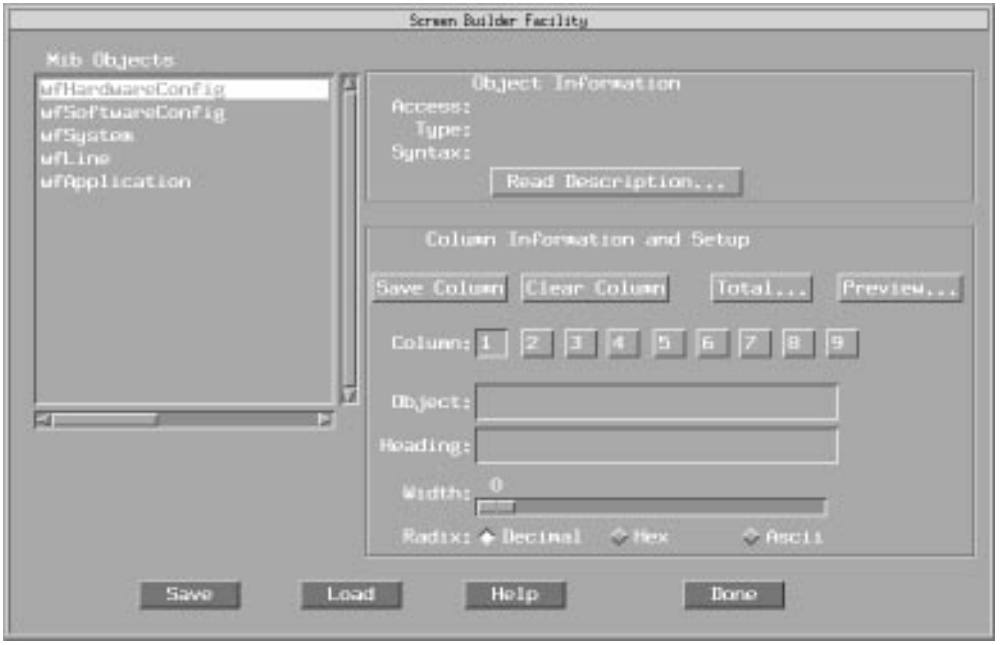

Figure 4-24. Screen Builder Facility Window

The MIB Browser on the left side of the screen lets you scroll through the MIB and select MIB objects to add to the screen. (The section "Using the MIB Browser," earlier in this chapter, explains how to maneuver through the MIB). The Column Information and Setup portion of the screen lets you specify how the statistics for the selected objects appear on the screen.

2. **Specify the column you want to define in the screen design by clicking on the corresponding column number.**

   For example, to define the first column on the statistics screen, click on the "1."

3. **Scroll through the MIB tree and select the MIB object that you want to list in the column.**

   The Object field in the Column Information and Setup portion of the screen displays the MIB object you select.

4. **Select the Heading field and enter a name that describes the type of statistics that the Statistics Manager will collect and display in that column.**

   For example, if you select the object wfIPInterfaceAddr, you could name the column "IP Address."

5. **Specify the column width. Click on the slidebar and move it back and forth until the Screen Builder displays the appropriate column width.**

   The width displays in character units. The width you specify here must be greater than 0 and greater than or equal to the column heading width. Any data that exceeds the specified column width will cause the rest of the data on the same line to shift to the right.

   As a rule of thumb, allow at least the following widths:

IP addresses	18 units (15 for the address, plus 3 spaces)
MAC addresses	16 units (14 for the address, plus 2 spaces)
Circuit Names/Numbers	18 units

6. **Specify whether the Statistics Manager displays statistics in decimal, hexadecimal, or ASCII format by clicking on the corresponding button in the Radix field.**

   You may find the ASCII radix useful for displaying NetBIOS Names.

7. **Click on Save Column to save the column attribute information.**

   The Screen Builder displays an asterisk in the column button for the column you just saved.

8. **Repeat Steps 1 to 7 to add other objects to the statistics screen.**

9. **To generate a sum of the values in two or more columns, follow these steps:**

   a. **Click on the number of the column in which you want to display the sum.**

   b. **Click on Total.**

      The Screen Builder Column Total window appears (Figure 4-25).

Figure 4-25. Screen Builder Column Total Window

   c. **Click on each column that will contain values that you want to include in a total.**

      For example, suppose Columns 1, 2, and 3 will contain information about different kinds of dropped packets. You can generate a total of all dropped packets by adding the values in the three columns.

      Figure 4-26 shows that Column 4 will display the total of the values in Columns 1, 2, and 3.

Figure 4-26. Selecting Columns to Total

d. Click on Save.

You then return to the Screen Builder Facility window.

e. Click on Save Column in the Screen Builder Facility window to save the totals column you just specified.

10. To preview the statistics screen you are building, click on Preview.

The statistics screen appears and displays the current column design. Note, however, that the Statistics Manager does not retrieve any statistics from the router.

11. Click on Save once you finish building the screen.

The Statistics Save/Load Screen window appears (Figure 4-27). It lists all the custom statistics screen files that you save in the statistics screen directory.

Figure 4-27. Statistics Save/Load Screen

12. Complete the Statistics Save/Load Screen as follows:

a. Enter a new name for the file in the Screen Name field.

If you are saving the file to a PC, the name you enter must follow standard DOS format.

b. Enter a description of the screen in the Description field.

The maximum length of the screen description is 40 characters.

c. Specify the screen mode by selecting either Circuit or Table.

Choose Circuit if you want the Statistics Manager to continually update the screen with new statistics. Choose Table if you want the Statistics Manager to gather and display current statistics only once, when you launch the screen.

d. Click on Save to save the statistics screen to a file.

Depending on whether you are running Site Manager on a UNIX or DOS computer, the Statistics Manager saves all custom screens to one of the custom screen directories listed:

Platform	Custom Screen Directory
UNIX	$(HOME)/.wfscrns
DOS	\wf\wfscrns

Displaying Custom Statistics Screens

To view a statistics screen you created, complete the following steps:

1. **Add the screen to the current screen list.**

   See "Defining the Current Screen List," earlier in this chapter, for instructions.

2. **Launch the screen.**

   See "Displaying Statistics Screens," earlier in this chapter, for instructions.

You can also view the text version of the statistics screen file using any text editor.

Editing Custom Statistics Screens

You can load a statistics screen that you previously built and edit the screen. This is a two-step procedure.

Note: *The default screens are write-protected, so you cannot edit them. To customize a default screen, simply use the operating system to copy it to the custom screen directory on your Site Manager workstation under a new name. Then load and edit it as described in this section.*

Retrieving a Statistics Screen File

Before you can edit a statistics screen file, you must load (retrieve) it from your Site Manager workstation.

To retrieve a statistics screen file, begin at the Statistics Manager screen and proceed as follows:

1. **Select Tools→Screen Builder.**

The Screen Builder window appears.

2. **Click on Load.**

   The Statistics Save/Load Screen appears.

3. **Highlight the statistics screen file you want to edit.**

   Once you select a statistics screen file, the Screen Information fields reflect the screen name and type of data it collects.

4. **Click on Load to load the screen's column attributes into the Screen Builder.**

The Column Information and Setup portion of the Screen Builder window now reflects the statistics screen you retrieved, beginning with the first column defined.

Editing a Statistics Screen File

After you retrieve the statistics screen, use the Screen Builder to edit the screen.

To edit the screen columns, follow these steps:

1. **Select the number box corresponding to the column you want to edit.**

   When you select the column number, the Object, Heading, Width, and Radix fields are filled in with the current column information. If the column is currently undefined, these fields remain blank.

   To remove all of the current column information, click on Clear Column.

2. **Select and edit any of the column attributes you want to change as follows:**

   — If you want the column to contain statistics about a different object, highlight a new object from the MIB Browser.

   — To change the column size, use the slidebar to increase or decrease the current size.

   — To change the column heading, type a new heading.

   — To display the integer in a different format, change the Radix setting.

   The section "Designing Statistics Screens," earlier in this chapter, describes how to set each of the column's attributes.

3. **Click on Save Column to implement your changes.**

4. **Repeat this procedure to edit additional columns.**

Note: *To display the statistics screen and see the results of your edits, click on Preview.*

5. **Click on Save to save your changes to the screen.**

   The Statistics Save/Load Screen appears. You can either save this modified window to an existing file or save it under a new name as follows:

   — To save the screen to an existing file, select the file from the list by highlighting it. Then click on Save. Click on OK to allow the Statistics Manager to overwrite the file.

   — To save the screen under a new name, enter the name of the file in the Screen Name field. Describe the file in the Description field, and specify whether the screen mode is Circuit or Table. Then click on Save.

If you save the statistics window under a new name, you must do the following to view this screen:

1. **Add the window to the current screen list.**

   See “Defining the Current Screen List” for instructions.

2. **Launch the screen.**

   See “Displaying Statistics Screens” for instructions.

Using the MIB II Counters Feature

MIB II is the second version of the Management Information Base. The MIB II Counters feature lets you track the number of packets each circuit in the Bay Networks router processes at the data link layer. By default, Site Manager enables the MIB II counters described in Table 4-2.

Table 4-2. MIB II Counters

Counter	Description
ifInNUcastPkts	Counts the number of nonunicast (such as subnetwork-broadcast or subnetwork-multicast) packets delivered to a higher-layer protocol.
ifOutUcastPkts	Counts the total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
ifOutNUcastPkts	Counts the total number of packets that higher-level protocols requested be transmitted to a nonunicast address, including those that were discarded or not sent.
ifInUcastPkts	Counts the number of subnetwork-unicast packets delivered to a higher-layer protocol.
ifInUnknownProtos	Counts the number of packets received via the interface that were discarded because of an unknown or unsupported protocol.

To access these counters in the MIB Browser, select wfApplication, wfDataLink, wfIfGroup, and then wfIfTable.

Note that if you want to measure packet count statistics at the data link layer, you should not disable the counters; doing so would result in inaccurate aggregate statistics. However, if you choose to disable the counters, you can do so by following these steps:

1. **In the Configuration Manager window, select Platform→MIB II Counters.**

   The MIB II Counters Enable/Disable window appears (Figure 4-28).

Figure 4-28. MIB II Counters Enable/Disable Window

2. **Click on Values and select Disable.**

   Note that disabling the counters disables them on all circuits and slots. Likewise, enabling the counters enables them on all circuits and slots.

3. **Click on OK to exit the window and save the change.**

For More Information

For information about MIB standards, see the following references:

Structure and Identification of Management Information for TCP/IP-based Internets (SMI; RFC 1155).

Information Processing Systems – Open Systems Interconnection Specification of Abstract Syntax Notation One (ISO 8824).

Chapter 5
Managing Router Files

For general information about managing router files, see “Managing Router Files” in Chapter 1. For specific information about using buttons, windows, and other Site Manager features, refer to *Using Site Manager Software*.

To manage router files, you can use the Router Files Manager to do the following:

- Display the contents of a router’s volume
- Connect to a router
- Name files
- Copy files
- Delete files
- Transfer files
- Back up files
- Modify a *config* file in remote configuration mode
- Compact file space on a memory card or flash SIMM
- Format a memory card or flash SIMM
- Partition media on Bay Networks routers

Displaying the Contents of a Volume

To display files stored on a volume inside the router, begin at the main Site Manager window and click on Files, or select Tools→Router Files Manager. The Router Files Manager window appears, showing the files in the active volume (Figure 5-1).

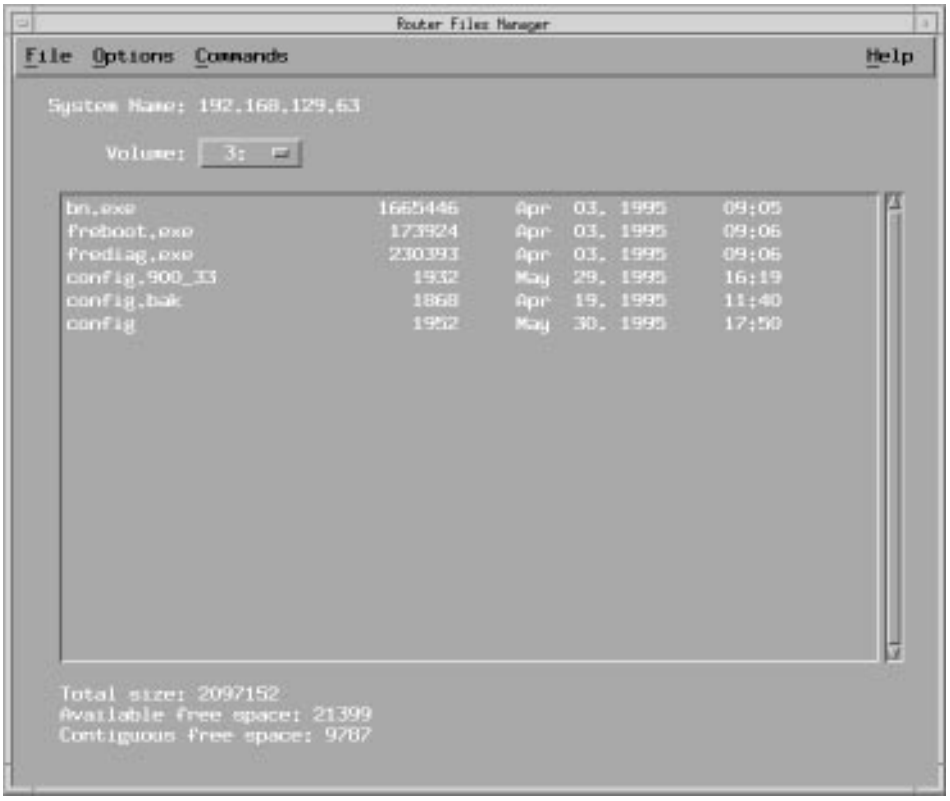
Router Files Manager
File Options Commands Help
System Name: 192.168.129.63
Volume: 3:
bn.exe 1665446 Apr 03, 1995 09:05
freboot.exe 173924 Apr 03, 1995 09:06
frediag.exe 230393 Apr 03, 1995 09:06
config.900_33 1932 May 29, 1995 16:19
config.bak 1868 Apr 19, 1995 11:40
config 1952 May 30, 1995 17:50
Total size: 2097152
Available free space: 21399
Contiguous free space: 9787

Figure 5-1. Router Files Manager Window

Active Volumes

In the Router Files Manager window, the active volume is represented by a number or letter, depending on the type of media the router uses. See Table 5-1.

Table 5-1. Active Volume Representations

Media	Active Volume	Description
Flash Memory Card or Memory Module	1 through 14*	If the router uses a memory card or a memory module, the active volume can be from 1 through 14, depending on the router platform.
Diskette	A	If the router uses a diskette, the active volume shown is A.

*. This number comes from the number of the slot hosting the first available memory card. Additional memory cards in the router are optional; they provide redundancy and additional storage.

In addition, if the router is an Access Node (AN) or Access Stack Node (ASN), and the media is partitioned, the active volume is represented by a number (for the slot) and a letter (for the volume). For example, 1A refers to volume A (the primary volume) on slot 1, and 1B refers to volume B (the secondary volume) on the same media in slot 1. For more information, see “Partitioning Media on Bay Networks Routers” later in this chapter.

To change the volume displayed, select the Volume box. The Volume box lists all available volumes on the router, as shown in Figure 5-2. Select the volume you want.

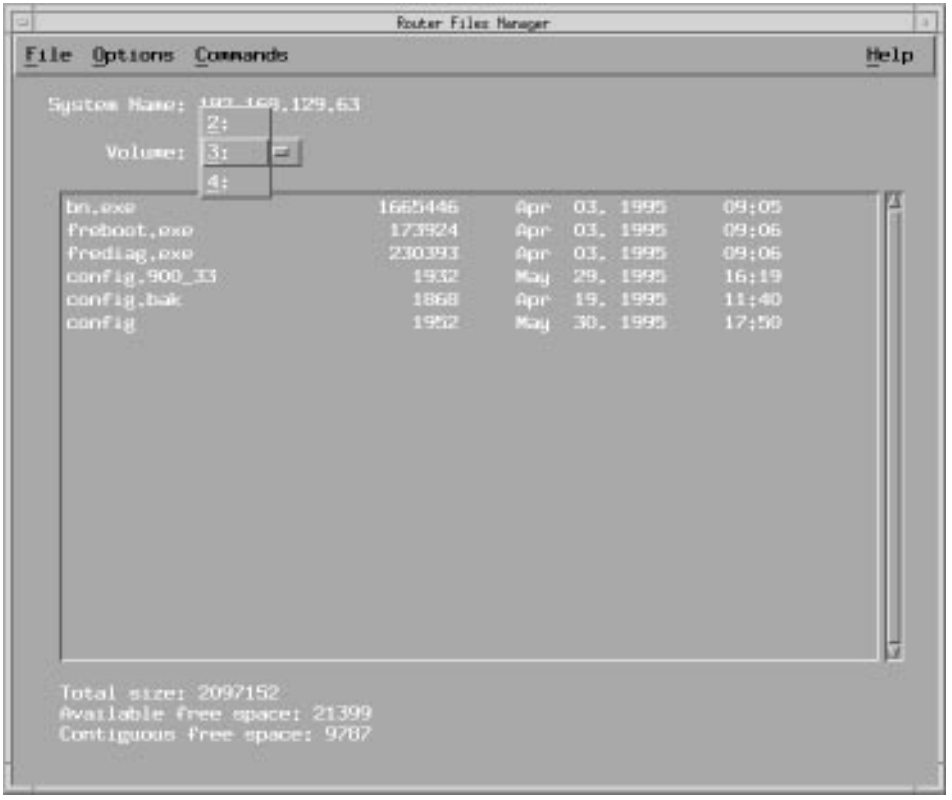

Figure 5-2. Volume Box in Router Files Manager Window

Available and Contiguous Free Space

The fields at the bottom of the Router Files Manager window show the amount of free space in a selected volume.

Table 5-2 describes the fields.

Table 5-2. Free Space Fields in Router Files Manager Window

Field	Description
Total size	Total number of bytes (used and unused) on the volume
Available free space	Number of unused bytes on the volume
Contiguous free space	Number of unused bytes in the largest block available on the volume

Default Filenames

Table 5-3 lists the default router filenames.

Table 5-3. Default Router Filenames

Filename	Description	Notes
ace.out	Bootable image for the FN, LN, ALN, AFN with diskette, and CN	The system automatically references this binary file for booting instructions, unless you specify another bootable image. You cannot read or change this file. It must have the correct filename for the system to boot successfully after a cold start. The Administration→Boot Router option does, however, let you specify another software image.
afn.exe	Bootable image for the AFN with flash file system	
an.exe	Bootable image for the AN	
asn.exe	Bootable image for the ASN	
bn.exe	Bootable image for the BLN, and BCN	
asndiag.exe	Copy of the diagnostics image for the ASN	You cannot read or change this file.
config	Default configuration file	The system references this binary file for configuration data when booting. (However, you can specify another configuration file with the Boot Router option.) You can change the configuration by copying an alternate configuration file to *config*. Also, you can store alternate or future configurations. This file must have the *config* filename for the system to configure automatically after booting. We recommend that you back up the *config* file before overwriting it.

(continued)

Table 5-3. Default Router Filenames *(continued)*

Filename	Description	Notes
debug.al	ASCII file containing aliases	Aliases are commands that abbreviate long or multiple commands. They are used to debug common network problems.
frediag.exe	Copy of the diagnostics image resident on the diagnostics PROM for the BCN and BLN	You cannot read or change this file.
freboot.exe	Copy of the bootstrap image resident on the bootstrap PROM for the BCN and BLN	You cannot read or change this file.
install.bat	Script containing Technician Interface commands	You use the Bay Networks Technician Interface commands during the initial startup.
ti.cfg	Configuration file containing the MIB variables associated with the default Technician Interface console operating parameters	This file contains the minimal configuration necessary to operate the router. You boot with this file when updating a PROM. You may also want to boot with this file when copying a volume to provide full use of all system buffers. This file is stored in binary format.

Note: *Although you cannot read or change the contents of bootable images (such as* an.exe *or* asn.exe*), you can rename these files. If you rename a bootable image file, you must specify the new name when you boot the router. See Chapter 7 for information on booting routers.*

Connecting to a Router

To connect to a router using the Router Files Manager:

1. **Select Options→Connections from the Router Files Manager window.**

   The Router Connection Options window appears (Figure 5-3).

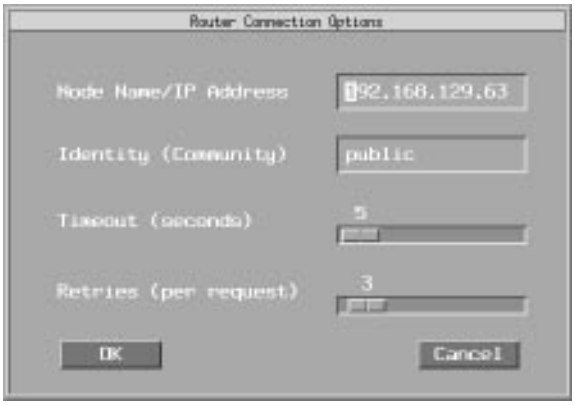

Figure 5-3. Router Connection Options Window

2. **Enter an IP address in the Node Name/IP Address field, then click on OK.**

   The Router Files Manager connects you to the specified router. The IP address of that router appears in the Router Files Manager window.

Naming a File

Before you continue with this section, you need to know the rules for naming files.

- Filenames must start with an alphabetical character. The remaining characters must be alphanumeric and may also include the underscore (_) character.
- Filenames can consist of 1 to 8 characters. Note that configuration filenames can consist of 1 to 15 characters (including a period). However, we recommend that you limit filenames to 8 characters to ensure that all operating systems that we support can recognize the names.
- Filename extensions are optional and must be preceded by a filename and a dot. They can be from 1 to 3 characters.

Also, we recommend that you use the following conventions when you name files so that you can distinguish files by type.

- Use the *.exe* filename extension for software images for FRE processor modules and *.out* for ACE processor modules. (See Table 5-3, earlier.)

- Use the *.cfg* filename extension for alternate configuration files. (The default configuration file is *config*.)
- Use the *.al* filename extension for alias files.
- Use the *.log* filename extension for log files.

Copying a File

You can use the Router Files Manager to copy a file on the router. You can copy the file to a different volume or to the same volume. To copy a file, you do the following:

1. **Examine the existing filenames.**
2. **Verify the existence of adequate free space on the destination volume.**
3. **Create the copy.**

The following sections describe each of these steps.

Examining the Router Destination Volume

The router automatically overwrites any file that has the same filename as the file you are creating.

To avoid overwriting an existing file, display a list of the volume's contents and determine the filenames that are already in use. For information on how to do this, see "Displaying the Contents of a Volume" earlier in this chapter.

If you are unfamiliar with the file-naming rules and conventions, refer to the earlier section "Naming a File" before you proceed.

Verifying Adequate Free Space

You must be certain that the router volume has enough space available for the copy. Depending on the router software version you are using, your software might automatically check the available space for you.

To determine your router software version, select Help→Site Manager Version in the Router Files Manager window.

Routers that run 7.80 (or later) software automatically make sure enough free space exists on the destination volume specified in a file copy operation.

For routers that use a software version earlier than 7.80, you must

- Determine from the Router Files Manager window the size of the file you want to copy.
- Determine from the Router Files Manager window the amount of free space available to receive the file copy on the destination volume:
  - For a router diskette destination volume, use the number of bytes displayed for `Available free space`.
  - For a router Flash memory card destination volume, use the number of bytes displayed for `Contiguous free space`.

Caution: *Copying a file to a memory card "volume" that has an insufficient amount of contiguous free space results in a corrupted copy of the original source file. You must delete the corrupted file.*

Before you again attempt to copy the same or any other source file(s) to the same volume, you must compact the volume. See "Compacting File Space on a Flash Memory Card " later in this chapter.

Creating the Copy

Copy a file as follows:

1. **In the Router Files Manager window, select the file you want to copy.**

   If you select a file that you decide not to copy, click on the file again to deselect it.

2. **Select Commands→Copy. The Router Files Manager displays the source filename in a window (Figure 5-4).**

Figure 5-4. Copy File Window for Source Filename

3. **Click on OK.**

   A window prompts you for the destination filename (Figure 5-5).

Figure 5-5. Copy File Window for Destination Filename

4. **Using the following format, overtype the entry in the Destination Filename field with the volume and filename you want to give this file.**

   <*volume*>:<*filename*>

Note: *If you are copying a file from diskette to memory card, enter the destination filename in lowercase letters only.*

5. **Click on OK.**

   A confirmation window appears.

6. **Click on OK.**

The router copies the source file to the filename and volume you specified.

Deleting a File

You can delete one or more files at a time from a volume.

Caution: *You cannot recover a file after it is deleted.*

To delete one or more files, follow these steps:

1. **In the Router Files Manager window, select each file that you want to delete.**

   To select multiple files, just click on each file you want.

   If you select a file that you decide not to delete, click on the file again to deselect it.

2. **Select Commands→Delete.**

   A window prompts you to confirm your delete request (Figure 5-6).

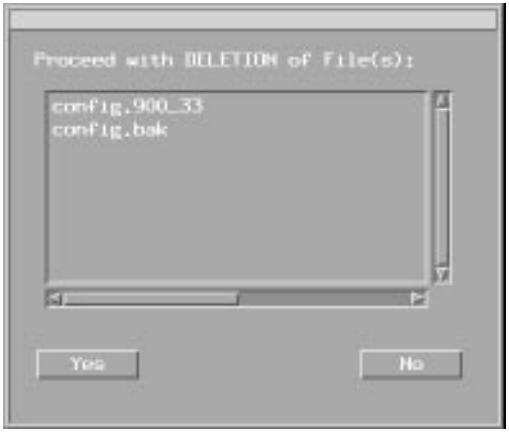

Figure 5-6. Deleting Router Files

3. **Click on Yes.**

The router deletes the files you specified from the volume displayed.

Transferring a File

The Router Files Manager allows you to transfer files between any router and Site Manager workstation by selecting File→TFTP (Figure 5-7).

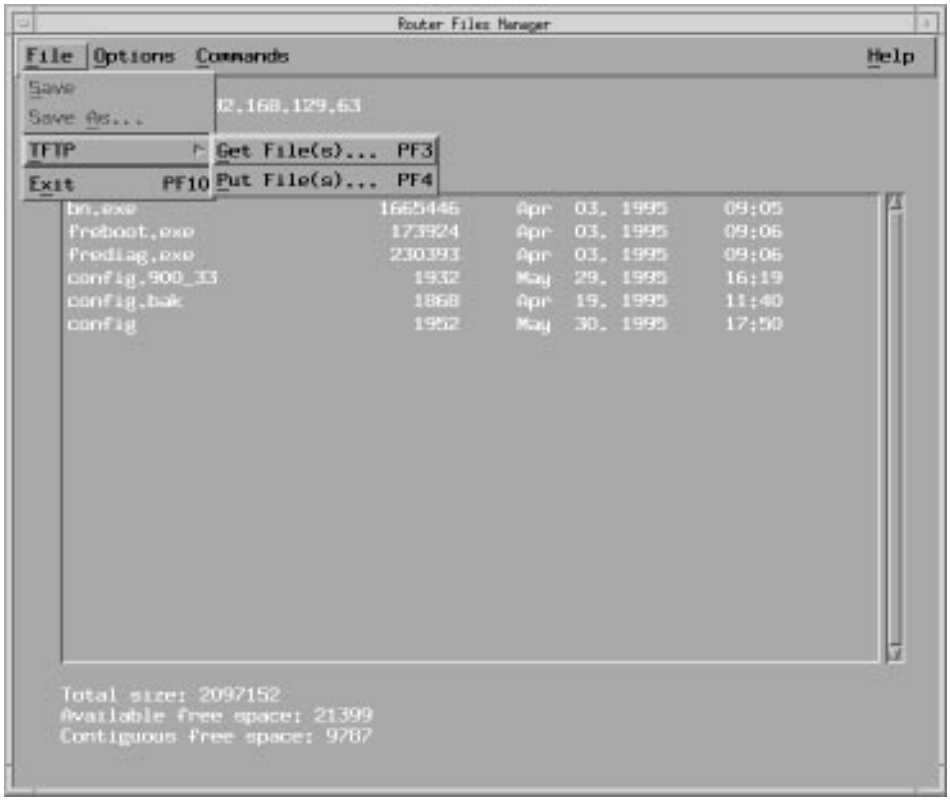

Figure 5-7. Selecting the TFTP Option

This option invokes the TFTP (Trivial File Transfer Protocol) software to execute file transfers.

Note: *To transfer files to or from a router that uses a diskette-based file system, you must set the TFTP Retry Time Out parameter to 10 seconds. If you do not make this adjustment, duplicate transfer sessions may occur. This, in turn, may result in zero length or locked files on the diskette. (For more information on how to set the TFTP Retry Time Out parameter, refer to* Configuring IP Services.*)*

You can choose TFTP→Put File(s) to transfer one or more files to several routers at the same time. For example, you might want to transfer a new boot image to three different routers. Rather than performing the transfer three times (once for each router), you can transfer the file to all three routers at once.

To transfer files to multiple routers simultaneously, you must use the Router Files Manager to set up those routers. The next section describes how to do this.

If you want to transfer files to only one router, the Router Files Manager uses the Node Name/IP Address that you specified in the Router Connection Options window to determine the router onto which you put files. For more information, see the section “Putting a File,” later in this chapter.

You can choose TFTP→Get File(s) to get one or more files from a router. Unlike the Put File(s) option, which lets you transfer files to several routers at the same time, you can get files from only one router at a time. Again, the Router Files Manager uses the Node Name/IP Address from the Router Connection Options window to determine the router from which to get files. For more information, see the section “Getting a File,” later in this chapter.

Note: *We recommend that you ping the router before you transfer a file, if you are running IP in host-only mode and you have configured the router with the same IP address on multiple physical interfaces.*

Setting Up Multiple Routers

To set up several routers so that you can put the same files on those routers at one time, follow these steps:

1. **Select Options→Router Connection and complete the Router Connection Options window for each router to which you want to transfer the files.**
2. **Select Options→ Multiple Router Setup.**

   The Multiple Router Setup window appears (Figure 5-8).

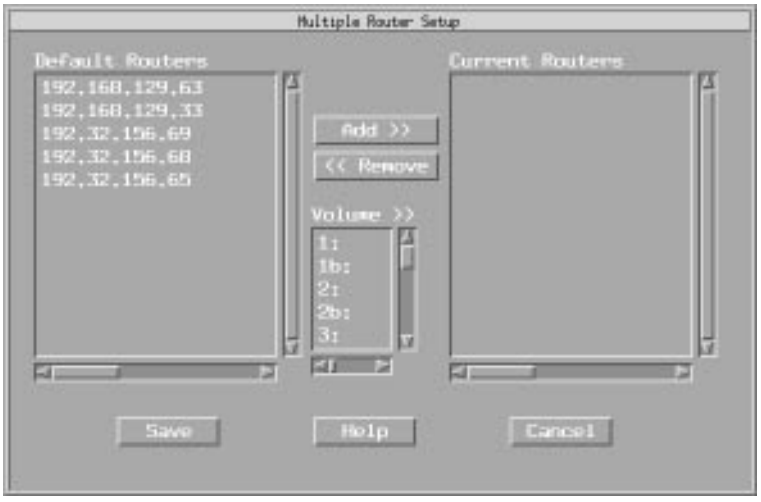

Figure 5-8. Multiple Router Setup Window

The Default Routers window lists the routers to which you are currently connected. The Current Routers window lists the routers whose files you want to manage simultaneously. The Volume window lists all of the volume identifiers for Bay Networks routers.

3. **To transfer files to the same volume(s) on several different routers, follow these steps:**

   a. **In the Default Routers list, click on each router to which you want to transfer the same files at the same time.**

   b. **In the Volume list, click on each volume where you want to put files.**

   c. **Click on Add.**

      The selected routers and volumes appear in the Current Routers list (Figure 5-9).

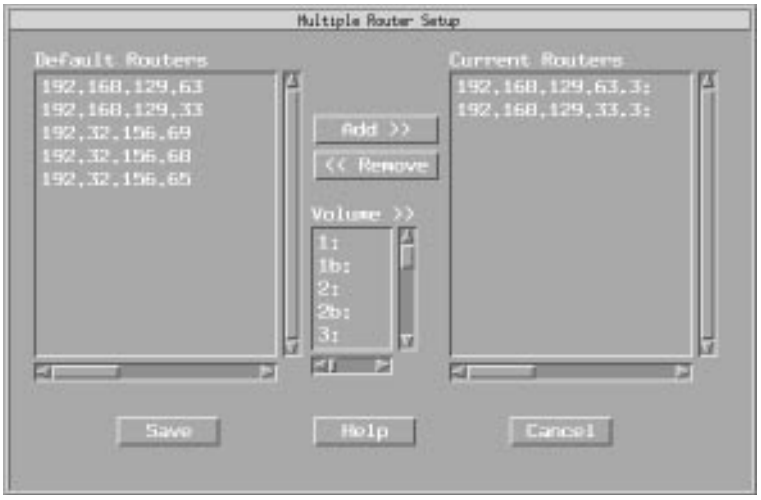

Figure 5-9. Adding Routers to the Current Routers List

Using the multiple router setup in Figure 5-9, you can transfer the same files to Volume 3 on each of the routers in the Current Routers list.

To transfer files to different volume(s) on several different routers, follow these steps:

a. **In the Default Routers list, click on the router to which you want to transfer files.**

b. **In the Volume list, click on the volume(s) where you want to put files on the router you just selected.**

c. **Click on Add.**

d. **Repeat Steps a through c for each router to which you want to transfer the same files.**

   The selected routers and volumes appear in the Current Routers list (Figure 5-10).

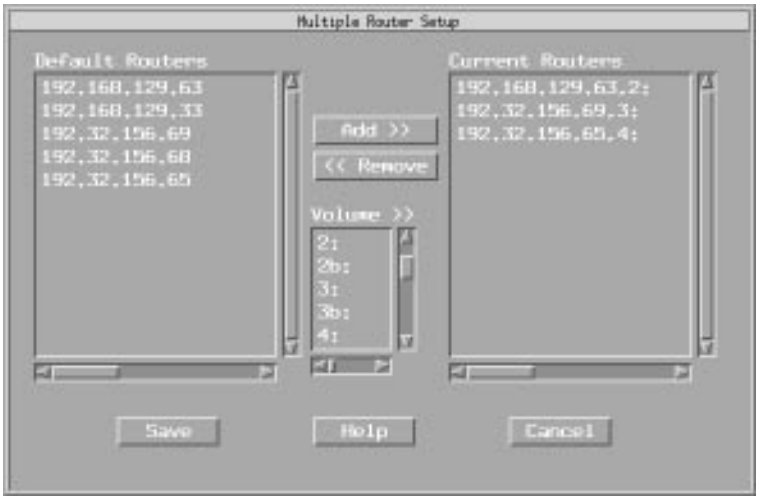

Figure 5-10. Multiple Router Setup Window

Using the multiple router setup window shown in Figure 5-10, you can transfer the same files to Volume 2 on the first router in the Current Routers list, Volume 3 on the second router in the list, and Volume 4 on the third router.

If you inadvertently add a router and volume to the Current Routers list, you can remove it from that list. To do so, select the router (in the Current Routers list) and click on Remove.

4. **Click on Save.**

You can now proceed to "Putting a File" for information on putting files on the routers.

Getting a File

The Get File option allows you to transfer one or more files from the router to the Site Manager workstation.

To transfer files from the router to the Site Manager workstation, begin at the Router Files Manager window and proceed as follows:

1. **Select Options→Router Connection from the Router File Manager window.**

2. **Enter the IP address of the router that has the files you want to transfer; then click on OK.**
3. **Select the router volume from which you need to transfer a file.**

   The Router Files Manager lists the files on that volume.
4. **Select the files you want to transfer from the router to the Site Manager workstation.**
5. **Select File→TFTP→Get File(s).**

   The TFTP Get Files window appears (Figure 5-11).

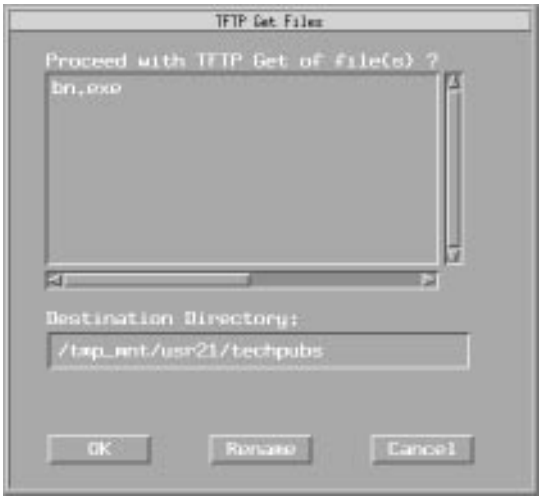

Figure 5-11. TFTP Get Files Window

In this example, you are transferring one file from the router to the Site Manager workstation.

6. **To store the file on your Site Manager workstation without changing the filename, follow these steps:**

   a. **In the Destination Directory field, enter the name of the directory on your Site Manager workstation where you want to store the file.**

   b. **Click on OK to proceed.**

      The Router Files Manager transfers the files to the Site Manager workstation. If a file with the same name already exists in the destination directory on the Site Manager workstation, the file you are "getting" overwrites it.

   To store the file under a new name on your Site Manager workstation, follow these steps:

   a. **Click on Rename in the TFTP Get Files window (Figure 5-11).**

      The TFTP Rename Files window appears (Figure 5-12).

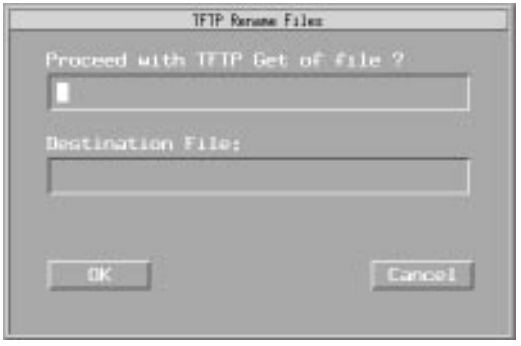

Figure 5-12. TFTP Rename Files Window

   b. **In the Proceed with TFTP Get of file field, enter the name of the file you want to retrieve from the router.**

   c. **In the Destination File field, type the path and filename under which you want to store the file on your Site Manager workstation.**

   d. **Click on OK.**

      The Router Files Manager transfers the files to the Site Manager workstation.

Putting a File

The Put File option lets you transfer files from the Site Manager workstation to one or more routers. To transfer a file from the Site Manager workstation to a router, you must do the following:

1. **Choose the router(s) to which you want to transfer the files.**
2. **Examine the existing filenames on the router destination volume.**
3. **Verify the existence of adequate free space on the destination volume.**
4. **Transfer the files to the destination volume.**

The following sections describe each of these steps.

Choosing the Routers

To transfer files to more than one router at a time, follow the instructions in the earlier section, "Setting Up Multiple Routers," to select the routers you want.

To transfer files to only one router, follow these steps from the Router Files Manager window:

1. **Select Options→Router Connection from the Router File Manager window.**
2. **Enter the IP address of the router to which you want to transfer files, then click on OK.**

Note: *We recommend that you ping the router before you attempt to transfer a file, if you are running IP in host-only mode on the destination router, and you have configured the destination router with the same IP address on multiple physical interfaces.*

Examining the Router Destination Volume

The router automatically overwrites any file that has the same filename as the file you are transferring from your Site Manager workstation.

To avoid overwriting an existing file on the router destination volume, display a list of the volume's contents and determine the filenames that are already in use. For information on how to do this, see "Displaying the Contents of a Volume" earlier in this chapter.

If you are unfamiliar with the file-naming rules and conventions, refer to the earlier section “Naming a File” before you proceed.

Verifying Adequate Free Space on the Destination Volume

You must be certain that the router destination volume has enough space available for the files you transfer. Depending on the router software version you are using, your software might automatically check the available space for you.

To determine your router software version, select Help in the Router Files Manager window.

Routers that run 7.80 (or later) software automatically verify the existence of adequate free space on the destination volume specified in a TFTP Put operation.

For routers that use a software version earlier than 7.80, you must

- Determine from the Router File Manager window the size of the file you want to transfer to the router via TFTP
- Determine from the Router File Manager window the amount of free space available to receive the file copy on the destination volume
  - — For a router diskette destination volume, use the number of bytes displayed for `Available free space`.
  - — For a router memory card or flash SIMM destination volume, use the number of bytes displayed for `Contiguous free space`.

Caution: *The destination volume may reside on a router that is running a version of the Series 7 software earlier than 7.80 (for example, 7.60). In this case, if the destination volume does not have enough free space (or contiguous free space, for a memory card volume), the router accepts only a partial (corrupted) copy of your source file.*

If you inadvertently transfer a file to a memory card volume that cannot accommodate your entire source file, delete the corrupted file copy from the destination volume. (See “Deleting a File” earlier in this chapter.) Before you transfer the same or any other source file(s) to the same volume, compact the contents of that volume. (See “Compacting File Space on a Memory Card or Flash SIMM” later in this chapter.)

Transferring Files to the Destination Volume

To transfer files from the Site Manager workstation to one or more routers, follow these steps from the Router Files Manager window:

1. **Select File→TFTP→Put File(s).**

   The TFTP Put File Selection window appears (Figure 5-13).

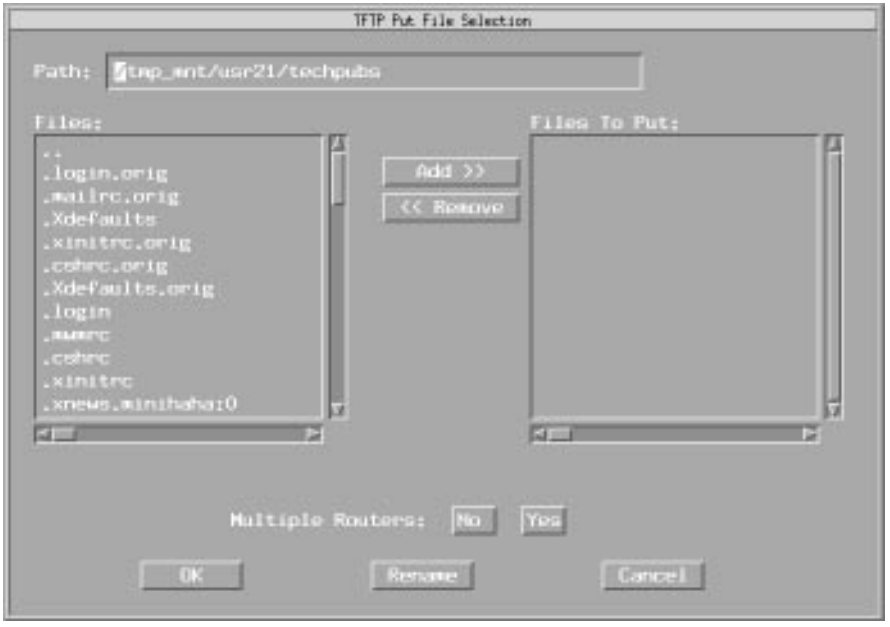

Figure 5-13. TFTP Put File Selection Window

2. **In the Path box, enter the pathname of the directory on the Site Manager workstation that contains the files you want to transfer.**

   The files in that directory appear in the Files window.

3. **In the Files window, click on each file that you want to transfer to the router. Then click on Add.**

   The selected files appear in the Files to Put window.

   If you inadvertently add files to the Files to Put window that you do not want to transfer to the router, select those files in the Files to Put window. Then click on Remove.

4. **Repeat Steps 2 and 3 to select files from other directories that you want to transfer to the router.**

5. **If you select multiple routers (see "Choosing the Routers" earlier in this section) and you want to transfer the files to all of the routers you selected, click on Yes in the Multiple Routers field.**

   If you select only one router, or if you do not want to transfer the files to all of the routers you set up in the Multiple Router Setup window, click on No in the Multiple Routers field. In this case, if you previously set up multiple routers, the Router Files Manager transfers the selected files only to the router to which you are currently connected.

6. **To transfer the files and store them on the router without changing the filenames, click on OK.**

   During the file transfer operation, the Router Files Manager displays the address of the router that is receiving the files. When the transfer (to each of the routers) is complete, the TFTP Put File Selection window closes and you return to the Router Files Manager window.

   To transfer a file and store it on the router under a different filename, follow these steps:

   a. **Click on Rename in the TFTP Put File Selection window.**

      The TFTP Rename Files window appears (Figure 5-14).

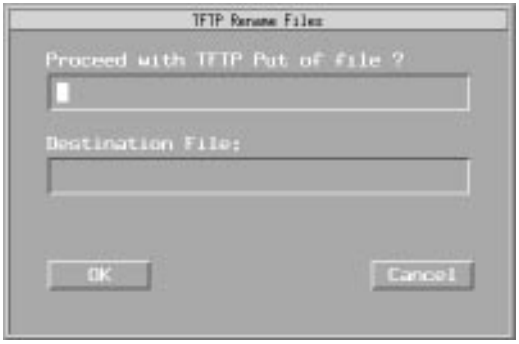

Figure 5-14. TFTP Rename Files Window

   b. **In the Proceed with TFTP Put of file field, enter the name of the file you want to transfer to the router.**

Do not enter the complete pathname, since you specified the pathname in the TFTP Put File Selection window.

c. **In the Destination File field, type the name under which you want to store the file on the router.**

d. **Click on OK.**

The Router Files Manager transfers the files to the Site Manager router to which you are currently connected. A message appears in the TFTP Rename Files window indicating when the operation is complete.

Note: *You can put a renamed file on only one router at a time (the router to which you are currently connected), even if you choose multiple routers in the TFTP Put File Selection window.*

e. **Click on Cancel in the TFTP Rename Files window.**

You return to the TFTP Put File Selection window. You can then click on OK to transfer any remaining files (without changing the filenames), or repeat these steps for each file you want to rename.

Backing Up Router Software Files to a Host Computer

We recommend that you use TFTP to back up the contents of each memory card or flash SIMM to a host computer on your network. After you back up all files, you can remove the files *freboot.exe* and *frediag.exe*. These files are not required on the router's memory card, flash SIMM, or diskette and are distributed only as backups for the EEPROMs.

Modifying *config* Files in Remote Configuration Mode

Use this procedure when you use the Configuration Manager remote mode to modify a *config* file.

1. **Compact the contents of the memory card or flash SIMM if your router is equipped with one.**

   See the next section, "Compacting File Space on a Memory Card or Flash SIMM."

2. **Copy the *config* file to a new file named *temp*.**

   See "Copying a File" earlier in this chapter.

3. **Modify *temp*, using the Configuration Manager remote mode.**

   Refer to the appropriate Bay Networks manual for customizing the type of router software you use.

4. **Save *temp*. When you save in remote mode, Site Manager automatically copies the file to the router.**

5. **To test your modifications, boot the router with the file *temp*.**

   Refer to "Booting a Router" in Chapter 7.

6. **Check the MIB version in the Site Manager main window. If the version is earlier than 7.80, verify that**

   — Adequate free space exists on the router's diskette to copy *temp* to another file

   — Adequate contiguous free space exists on the router's memory card or flash SIMM to copy *temp* to another file

Note: *Routers that run 7.80 (or later) software automatically verify the existence of adequate free space on the destination volume specified in a file copy operation.*

7. **Copy the file temp to *config*.**

8. **Boot the router with *config*.**

9. **Delete *temp*.**

Compacting File Space on a Flash Memory Card

Note: *References to memory cards in this section also apply to flash SIMMs (Single Inline Memory Modules) and PCMCIA SRAM cards (used with BNX software).*

You must compact the memory card to ensure that the available free space is contiguous. When you delete a file on a memory card, the file becomes inaccessible, but the data remains on the memory card.

Eventually all space is used. The Compact option copies the active files from the memory card to the router's memory, erases the memory card, and copies the files back to the memory card.

This procedure gives you more file space, provided that you have more available free space than contiguous free space. (For more information, refer to “Available and Contiguous Free Space” earlier in this chapter).

Before you use the Compact option, you should be aware of the following:

- We recommend that you back up the files by copying them to a second memory card.
- You should compact file space at off-peak hours if possible, due to the resource requirements for performing the compaction.

To compact the files on a memory card, begin at the Router Files Manager window and proceed as follows:

1. **Select the volume that contains the memory card you want to format.**
2. **Select Commands→Compact.**

   A confirmation window appears.
3. **Click on OK.**

While the operation is in progress, a running percentage of work completed appears next to the Volume field in the Router Files Manager window. The router is unavailable for any other file system requests until it completes the compacting procedure.

Upon completion of the compacting operation, the Router Files Manager automatically displays the list of files stored in the memory card. If you issue a file system request before the router finishes compacting all files on the designated volume, the message `Last command failed` appears. (The router did not successfully complete the command.)

Caution: *During the compacting operation, if the slot that contains the memory card resets, runs diagnostics, or loses power, the memory card loses all its data and can become corrupted. Likewise, if you remove a memory card while it is being compacted, the memory card can become corrupted and lose its stored data.*

On AN routers, the compacting operation can take up to 12 minutes. Refrain from resetting the AN during this time. Resetting the AN during compacting will corrupt the memory card, and the AN will not boot until you replace the memory card.

Formatting a Memory Card or Flash SIMM

Note: *References to memory cards in this section also apply to flash SIMMs (Single Inline Memory Modules).*

The Format option allows you to format and initialize a memory card. Use the Format option to format new memory cards, if you did not obtain them from Bay Networks.

Caution: *You cannot recover files from a memory card after you use the Format option. We recommend that you copy them to a second memory card before you use the Format option.*

To format a volume, begin at the Router Files Manager window and proceed as follows:

1. **Select the volume that contains the memory card you want to format.**
2. **Select Commands→Format.**

   A confirmation window appears.
3. **Click on OK.**

   The router formats and initializes the memory card.
4. **Display a list of the volume's contents when the format operation is done.**

The format process is complete if the Router Files Manager does not display a list of files.

Partitioning Media on Bay Networks Routers

Site Manager lets you partition the nonvolatile file system (NVFS) on Bay Networks Access Nodes (ANs) or Access Stack Nodes (ASNs). These routers use a single flash file system; that is, the routers have only one medium where the file system resides. The NVFS for the AN resides on a Single Inline Memory Module (SIMM). The ASN uses a flash memory card. (You can stack ASNs and use more than one flash memory card in the stack to achieve file system redundancy. In this case, partitioning would not be necessary.) If the single flash file system fails, the router has no backup file system from which to boot.

Partitioning the file system divides it into two independent volumes of equal size. You can store default boot images and configuration files on each volume for redundancy. Then, if the router is unable to boot from the primary file system, it automatically attempts to boot from the secondary (or backup) file system.

For example, suppose the NVFS for your Access Node resides on a 4-MB SIMM. Partitioning the file system creates two 2-MB volumes. The volumes function independently, and you reference them with unique slot and volume identifiers. You could then copy the files from the primary volume to the secondary volume.

Note: *You can partition file systems on 4-MB media only.*

Creating a Partition

To partition the NVFS on an AN or ASN, follow these steps:

1. **In the Router Files Manager window, select the volume you want to partition. Make sure the value for** `Contiguous free space` **is no more than half of the volume's total size.**

   To create volumes of equal size, the existing file system cannot be more than half of the total media size. If the file system is too large, you might want to do one or more of the following so that you will be able to create a partition:

   — Format the media, as described in the previous section.

   — Delete some files, as described in "Deleting a File" earlier in this chapter.

   — Compact the files, as described in "Compacting File Space on a Memory Card or Flash SIMM" earlier in this chapter.

2. **If you want to partition the file system on an ASN, make sure that the flash memory card is not write-protected. (By default, we ship memory cards unprotected.)**

   See *Installing and Maintaining ASN Routers and BNX Platforms* for information on setting the Read/Write switch on the flash memory card.

3. **Select Commands→Create Partition**

   A window appears prompting you to confirm your decision to partition the media (Figure 5-15).

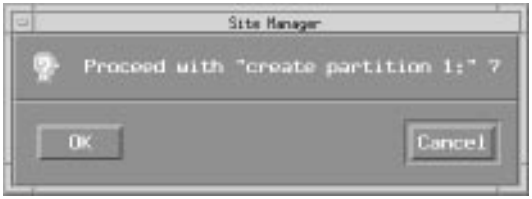

Figure 5-15. Create Partition Confirmation Window

4. **Click on OK in the confirmation window.**

   Site Manager displays the following message beside the volume box in the Router Files Manager window:

   ```
   CREATING media partition. Please wait...
   ```

   When the process is complete, the following message appears:

   ```
   Media partition created. Issuing DIRECTORY command.
   ```

The partitions function as independent flash media. Site Manager uses the following format to identify the partitions:

<*slot*><*volume*>**:**

where *slot* refers to the number of the processor board that contains the partitioned media, and *volume* is **a** for the primary volume and **b** for the secondary volume.

In the AN, the slot is always **1**. In an ASN, the slot can be from **1** to **4**, depending on the setting of the Slot ID selector. (See *Installing and Maintaining ASN Routers and BNX Platforms* for information on setting the slot ID.) For example, suppose you partition an AN's file system. Site Manager refers to the primary volume as **1a** and the secondary as **1b** (Figure 5-16).

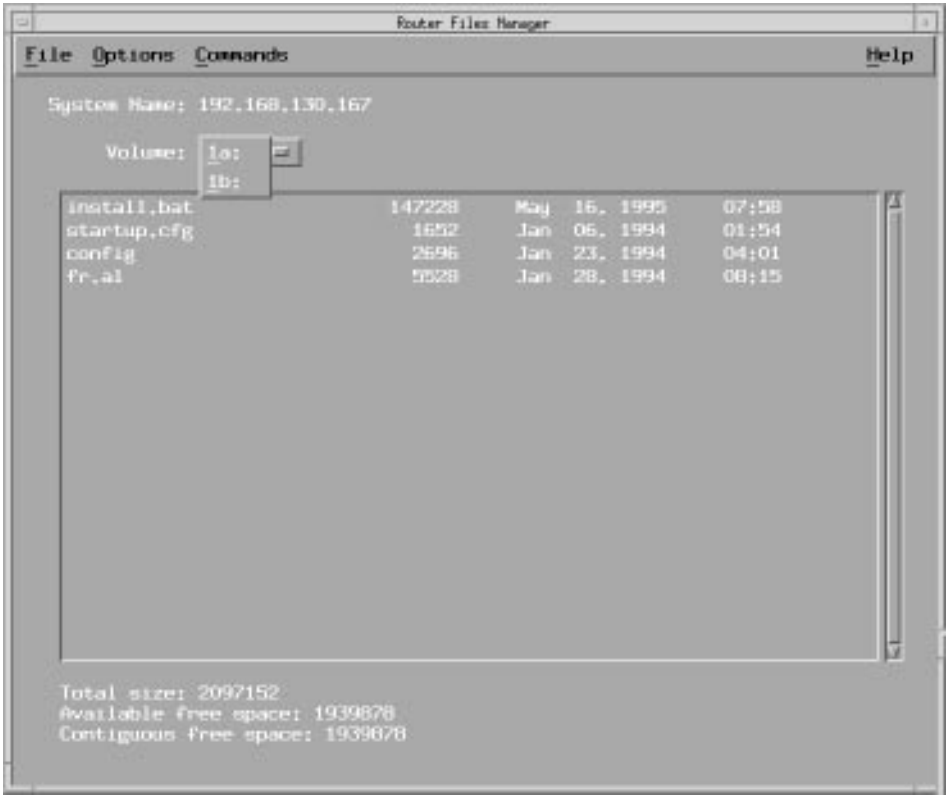
Router Files Manager
File Options Commands Help
System Name: 192.168.130.167
Volume: 1a: 1b:
install.bat 147228 May 16, 1995 07:58
startup.cfg 1652 Jan 06, 1994 01:54
config 2696 Jan 23, 1994 04:01
fr.al 5528 Jan 28, 1994 08:15
Total size: 2097152
Available free space: 1939878
Contiguous free space: 1939878

Figure 5-16. Volume Identifiers for Partitioned Media

To manage the files on a partitioned volume, you can use any of the commands that you would normally use to manage the files on an unpartitioned volume. For example, you can compact the files on one volume without affecting the files on the other.

You can use Command→Copy to copy the router files to the new volume. See "Copying a File" earlier in this chapter.

Note: *In partitioning the volume, the router creates a special partition file in the secondary volume. (You will not see the file in the secondary volume's list of files.) The partition file takes up 98 bytes of space in the secondary volume only.*

Deleting a Partition

If you partitioned the NVFS on your AN or ASN, you can remove the partition to revert to a single flash file system. You might want to do this, for example, if the router software image is larger than half of the total media size.

Caution: *Deleting a partition deletes all files from the secondary volume. Files on the primary volume remain intact, and the primary volume then represents the entire size of the medium.*

To delete a partition, follow these steps:

1. **In the Router Files Manager, click on the Volume box and switch to the primary volume.**
2. **Select Commands→Delete Partition.**

   A window appears prompting you to confirm your decision to delete the partition (Figure 5-17).

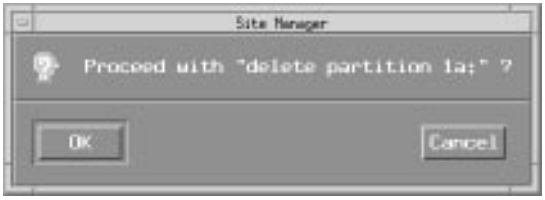

Figure 5-17. Delete Partition Confirmation Window

3. **Click on OK in the confirmation window.**

   Site Manager displays the following message beside the volume box in the Router Files Manager window:

   ```
   DELETING media partition. Please wait...
   ```

   When the process is complete, the following message appears:

   ```
   Media partition deleted. Issuing DIRECTORY command.
   ```

Chapter 6
Using the Report Generator and Audit Trail Feature

For general information about tracking router configuration file changes, see "Monitoring Changes to Router Configuration Files" in Chapter 1. For specific information about using buttons, windows, and other Site Manager features, refer to *Using Site Manager Software*.

You can monitor changes to router configuration files by doing the following:

- Generating configuration file reports
- Maintaining an audit trail log

Generating Configuration File Reports

You can generate reports from a router's configuration file from

- Site Manager
- The UNIX command line
- Windows on a PC

The following sections describe each method.

Generating Reports from Site Manager

To generate a configuration file report from Site Manager, select Tools→Report Generator from the Site Manager main window. The Configuration Report Generator window appears. Figure 6-1 shows a sample window.

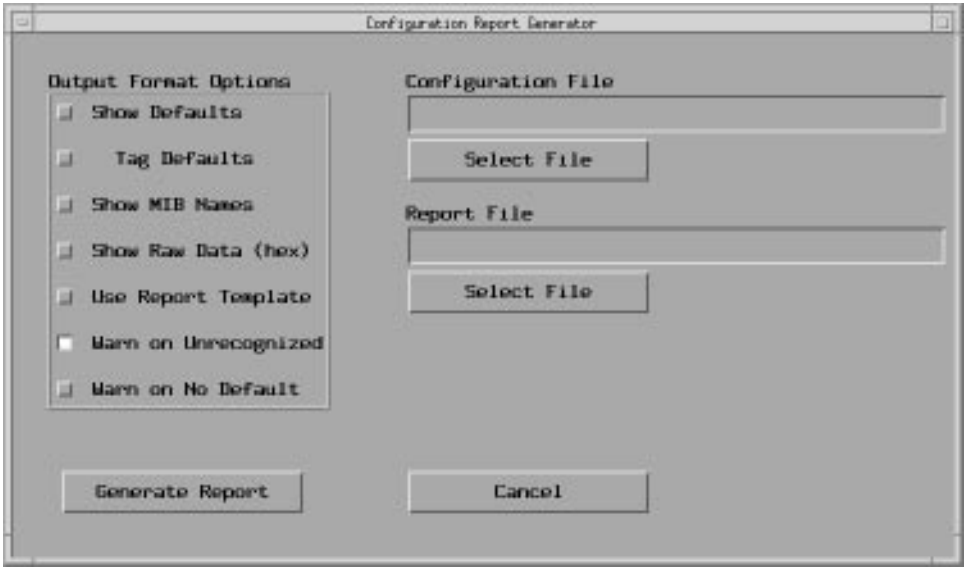

Figure 6-1. Configuration Report Generator Window

To complete the Configuration Report Generator Window, follow these steps:

1. **Select the Output Format Options that you want to use in the report.**

   To select an option, simply click in its box. Table 6-1 describes each option.

Table 6-1. Output Format Options

Option	Description
Show Defaults	Includes the MIB default value for any configurable attribute for which you did not specify a value in the configuration file.
Tag Defaults	Includes the label "[default]" beside any attribute that uses the MIB default value. If you click on Tag Defaults while Show Defaults is not selected, Site Manager automatically selects Show Defaults as well.
Show MIB Names	Includes MIB attribute identifier names in addition to the ASCII translation of those names.

(continued)

Table 6-1. Output Format Options *(continued)*

Option	Description
Show Raw Data (hex)	Includes the raw hexadecimal configuration data along with the ASCII translation of that data. You might want to show the raw data if you intend to use the Technician Interface to enter configuration data. In the Technician Interface, you must enter the data in raw format.
Use Report Template	Indicates that you want to use a report template other than the default. The default is a version-specific template based on the version of the configuration file. For example, the report generator uses a 7.80 template file to generate a report of a 7.80 configuration file. You might want to use a different report template, for example, a 7.60 template, to generate a report of a 7.80 configuration file. If you select this option, the Report Template File field appears below the Report File field in the Configuration Report Generator window. You must enter a filename in the Report Template File field, as described later.
Warn on Unrecognized	Includes the warning “Unrecognized Attribute” for any attribute that is in the configuration file but is not present in the MIB.
Warn on No default	Includes the warning “NO VALUE, NO DEFAULT” for any attribute for which you did not specify a value in the configuration file and that does not have a MIB default value.

2. **Click on Select File under the Configuration File field.**

   The Select Configuration File window appears (Figure 6-2).

Figure 6-2. Select Configuration File Window

Complete the Select Configuration File window as follows:

a. **In the Directories window, select the directory path that contains the configuration file from which you want to generate a report.**

b. **In the Files window, select the configuration file.**

   The pathname and filename appear in the Selection window.

c. **Click on OK.**

   You return to the Configuration Report Generator window.

3. **Click on Select File under the Report File field.**

Note: *You can skip this step if you want the Report Generator to send the output to* <stdout>.

The Save Report File As window appears (Figure 6-3).

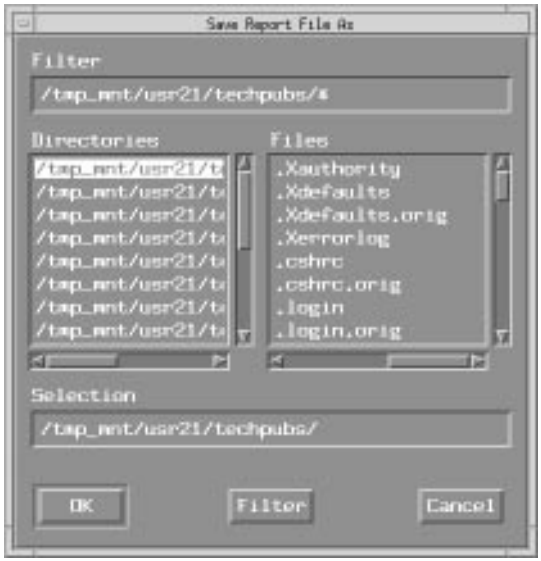

Figure 6-3. Save Report File As Window

Complete the Save Report File As window as follows:

a. **In the Directories window, select the directory path where you want to store the configuration file report.**

   The path appears in the Selection window.

b. **Enter a filename for the report after the path in the Selection window.**

c. **Click on OK.**

   You return to the Configuration Report Generator window.

4. **If you select Use Report Template in the list of Output Format Options, the Report Template File field appears in the Configuration Report Generator window. Click on Select under the Report Template File field.**

   The Report Template File window appears (Figure 6-4).

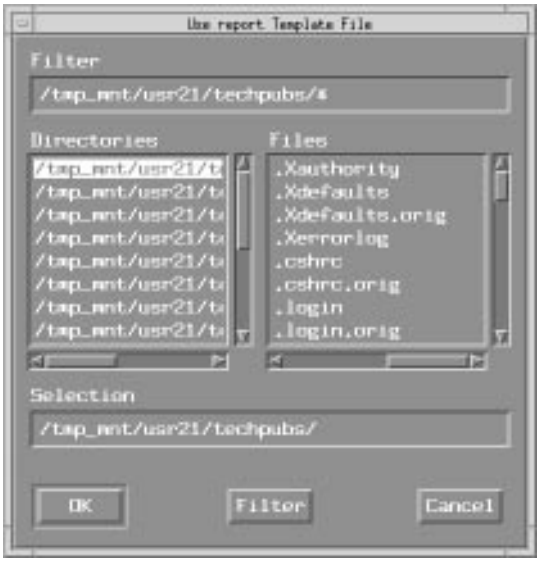

Figure 6-4. Use Report Template File Window

Complete the Use Report Template File window as follows:

a. **In the Directories window, select the directory path that contains the template file you want to use.**

b. **In the Files window, select the template file you want.**

   On UNIX workstations, template files are in */usr/wf/lib*. On PCs, the template files are in *c:\wf\lib*. The format of the template filename is

   <*version*>**.rpt**

   For example, the template file for the Version 7.80 configuration file is *7_80.rpt*.

   The pathname and filename appear in the Selection window.

c. **Click on OK.**

   You return to the Configuration Report Generator window.

5. **Click on Generate Report.**

Site Manager generates the configuration file report and saves the report under the filename you selected. You can then open the report in a text editor.

Figure 6-5 shows part of a report.

cmdtool (CONSOLE) - /bin/csh
Report produced by smcfgrpt Version <2.10>
date: Mon Jun 12 12:08:21 1995
configuration file: /extra/smgr/bruce/new.cfg
Router Software/MIB Version <8.10>
Hardware Configuration Group (wfHwBase)
Backplane Id (wfHwBpIdOpt) = Backbone Link Node (BLN)
wfHwEntry Table
wfHwEntry Entry
wfHwSlot<ID> = 3
Module Type (wfHwModIdOpt) = QENF
wfHwEntry Entry
wfHwSlot<ID> = 4
Module Type (wfHwModIdOpt) = 256--INVALID VALUE--
wfHwEntry Entry
wfHwSlot<ID> = 5
Module Type (wfHwModIdOpt) = SYNC
Protocols Configuration Group (wfProtocols)
IP loaded on slots (wfIPROTOLoad) = 3, 4
DLS loaded on slots (wfDLSLoad) = 3, 4, 5
TFTP loaded on slots (wfTFTPLoad) = None
SNMP loaded on slots (wfSNMPLoad) = None
TCP loaded on slots (wfTCPLoad) = 3, 4
LLC2 loaded on slots (wfLLC2Load) = 3, 4
NBASE loaded on slots (wfNBASELoad) = 5
SDLC loaded on slots (wfSDLCLoad) = 5
wfPingLoad = 4294705152
APPN Control Point loaded on slots (wfAPPNCpLoad) = 5
APPN Link Services loaded on slots (wfAPPNLsLoad) = 5
ARP loaded on slots (wfARPLoad) = None
Link Modules Configuration Group (wfLinkModules)
QENET loaded on slots (wfQENETLoad) = 3
QSYNC loaded on slots (wfQSYNCLoad) = 5
DT loaded on slots (wfDTLoad) = 4
Drivers Configuration Group (wfDrivers)
ILACC loaded on slots (wfILACCLoad) = 3
TM5380 loaded on slots (wfTM5380Load) = 4
MK5025 loaded on slots (wfMK5025Load) = 5
Switch Options Parameters Table
Switch Options Parameters Entry (wfCircuitNameEntry)
wfCircuitNumber<ID> = 1
wfCircuitNameDelete = 1
--More--

Figure 6-5. Sample Configuration File Report

Generating Configuration File Reports from UNIX

You can generate a configuration file report from the UNIX command line. The format of the UNIX command you use is as follows:

smcfgrpt [**-d**] [**-t**] [**-h**] [**-m**] [**-W** <*warning level*>] [**-r** <*report template*>] [**-c**] <*configuration file*> [[**-o**] <*report file*>]

Table 6-2 describes the options you can use in the UNIX command line.

Table 6-2. Options for Command Line (UNIX)

Option	Description
-d	Includes the MIB default value for any configurable attribute for which you did not specify a value in the configuration file.
-t	Produces the same result as **-d**, except that default values are tagged "[Default]."
-h	Includes raw hexadecimal data in addition to the ASCII translation of that data.
-m	Includes the MIB attribute identifier names in addition to the ASCII translation of those names.
-W <*warning level*>	Sets the warning level to indicate types of warnings to include in the report: 0 = no warning (default warning level) 1 = warn on unrecognized attributes 2 = warn on unrecognized records 3 = combination of levels 1 and 2 4 = warn on unset attributes with no default 7 = combination of 3 and 4
-r <*report template*>	Specifies the report template file to use. By default, the Report Generator uses a version-specific template based on the version of the configuration file. Template files are in */usr/wf/lib*. The format of the template filename is <*version*>**.rpt**. For example, the template file for the Version 7.80 configuration file is *7_80.rpt*.

(continued)

Table 6-2. Options for Command Line (UNIX) *(continued)*

Option	Description
-c <*configuration file*>	Specifies the name of the configuration file from which you want to generate a report.
-o <*report file*>	Specifies the pathname of the report file. If you omit this argument, the Report Generator sends the output to <*stdout*>.

Generating Configuration File Reports from Windows

You can generate a configuration file report from Windows on a PC. To do so, follow these steps:

1. **Bring up Windows on your PC.**
2. **Select File→Run.**

   The Run window appears.
3. **In the Command Line field of the Run window, enter the smcfgrpt command in the following format:**

   smcfgrpt [**-d**] [**-t**] [**-h**] [**-m**][**-W** <*warning level*>] [**-r** <*report template*>] [**-c**] <*configuration file*> [**-o**] <*report file*>

   Table 6-3 describes the options you can use in this command line.
4. **Click on OK in the Run window.**

Table 6-3. Options for Command Line (Windows)

Option	Description
-d	Includes the MIB default value for any configurable attribute for which you did not specify a value in the configuration file.
-t	Produces the same result as **-d**, except that default values are tagged “[Default].”
-h	Includes raw hexadecimal data in addition to the ASCII translation of that data.
-m	Includes the MIB attribute identifier names in addition to the ASCII translation of those names.

(continued)

Table 6-3. Options for Command Line (Windows) *(continued)*

Option	Description
-W <*warning level*>	Sets the warning level to indicate types of warnings to include in the report: 0 = no warning (default warning level) 1 = warn on unrecognized attributes 2 = warn on unrecognized records 3 = combination of levels 1 and 2 4 = warn on unset attributes with no default 7 = combination of 3 and 4
-r <*report template*>	Specifies the report template file to use. By default, the Report Generator uses a version-specific template based on the version of the configuration file. Template files are in *c:**wf**lib*. The format of the template filename is <*version*>**.rpt**. For example, the template file for the Version 7.80 configuration file is *7_80.rpt*.
-c <*configuration file*>	Specifies the name of the configuration file from which you want to generate a report. If the path to the configuration file is not in your PATH statement, be sure to enter the full pathname.
-o <*report file*>	Specifies the pathname of the report file.

For More Information

For information about converting your ASCII configuration file reports into bootable binary configuration files, refer to Appendix C.

Maintaining an Audit Trail Log

To use the Audit Trail feature, you must edit the default audit trail configuration file that comes with Site Manager. You edit the file to

- Specify an audit trail community; that is, the routers for which you want to create audit trail log files.
- Specify whether you want auditing on or off. By default, the Audit Trail feature is off.

The following section describes how to edit the audit trail configuration file.

Editing the Audit Trail Configuration File

Site Manager provides a default audit trail configuration file, *audit.cfg*. The file resides in */usr/wf* on UNIX workstations, and in *c:\wf* on PCs. You must edit the file to specify the following for each router you want to audit:

- The IP address of the router
- The pathname of the audit trail log file
- The email addresses of all users that the Audit Trail feature should notify if the router's configuration file changes
- Whether the audit trail feature is on or off

To edit the audit trail configuration file, follow these steps:

1. **To edit the audit trail configuration file on a UNIX workstation, copy the *audit.cfg* file to a directory where you have write permission.**
2. **Open *audit.cfg* in a standard text editor.**

   Figure 6-6 shows the default file.

```
#ROUTER=192.32.156.66
#AUDIT=ON
#FILE=/usr/wf/routerA.adt
#EMAIL=jdoe@wellfleet.com,jsmith@wellfleet.com
```

Figure 6-6. Default Audit Trail Configuration File

3. **Copy the four default lines in the file and insert them at the end of the file.**
4. **Delete the pound sign (#) at the beginning of the ROUTER= line. After the equal sign, overwrite the default value with the IP address of the router you want to audit.**

   For example, you might type

   ROUTER=**192.32.156.3**

5. **Delete the pound sign at the beginning of the FILE= line. After the equal sign, overwrite the default value with the pathname and filename for the audit trail log file for the router.**

   On UNIX workstations, the path for your audit trail log file should point to a directory in your UNIX environment where you have write permission. On PCs, the path is *c:\wf*. The filename should be the router's name (not its IP address) followed by the *.adt* extension.

   For example, you might type

   FILE=**/usr1/jb/southcape.adt**

6. **Delete the pound sign at the beginning of the EMAIL= line. After the equal sign, overwrite the default value with the email addresses of users you want to notify of configuration changes. Use a comma to separate each email address.**

   For example, you might type

   EMAIL=**pgrant,llantz,odiaz**

   If you do not want to use mail notification, delete the pound sign at the beginning of the EMAIL= line and delete the default email addresses.

Note: *The mail notification feature is not available on PCs.*

7. **Delete the pound sign at the beginning of the AUDIT= line. To enable audit trail logging, leave the default value, ON. To disable audit trail logging, type off after the equal sign.**
8. **Repeat Steps 2 through 6 for each router that you want to audit.**
9. **Save your changes and exit the file.**

You must specify the new pathname for the AUDIT_PATH environment variable. For UNIX platforms, this variable should point to the directory where you have placed the modified audit trail configuration file. For example:

```
AUDIT_PATH=/usr1/jake/audit.cfg
```

For the PC, the variable should point to the directory *c:\wf\audit.cfg*. For example:

```
set audit_path=c:\wf\audit.cfg
```

Viewing an Audit Trail Log File

Once Site Manager creates an audit trail log file and appends information to it, you can open it in any standard text editor. You can also print the file. Figure 6-7 shows a sample audit trail log file.

```
Wed Jul  6 04:57:13 1994
 192.32.156.71 wfSerialPortTable.11=2 ksnow remote.
Wed Jul  6 04:57:13 1994
 192.32.156.71 wfSerialPortTable.11=15 ksnow remote.
Wed Jul  6 04:58:37 1994
 192.32.156.71 wfSoftwareConfig.20=4 ksnow remote.
Wed Jul  6 04:58:37 1994
 192.32.156.71 wfSoftwareConfig.30=5 ksnow remote.
Wed Jul  6 04:58:37 1994
 192.32.156.71 wfSoftwareConfig.30=1 ksnow remote.
Wed Jul  6 04:58:37 1994
 192.32.156.71 wfCSMACDTable.16.2=6 ksnow remote.
Wed Jul  6 04:58:37 1994
 192.32.156.71 wfLineMappingTable.1106102=4 ksnow remote.
Wed Jul  6 04:58:37 1994
 192.32.156.71 wfLineMappingTable.1106102=3 ksnow remote.
Wed Jul  6 04:58:37 1994
 192.32.156.71 wfCSMACDTable.16.2=38 ksnow remote.
Wed Jul  6 04:58:37 1994
 192.32.156.71 wfCircuitNameTable.12=3 ksnow remote.
Wed Jul  6 04:58:37 1994
 192.32.156.71 wfCircuitNameTable.12=4 ksnow remote.
Wed Jul  6 04:58:37 1994
 192.32.156.71 wfCircuitNameTable.12=5 ksnow remote.
Wed Jul  6 04:58:37 1994
 192.32.156.71 wfCircuitNameTable.12=6 ksnow remote.
Wed Jul  6 04:58:37 1994
 192.32.156.71 wfCircuitNameTable.12=7 ksnow remote.
Wed Jul  6 04:58:37 1994
```

Figure 6-7. Sample Audit Trail Log File

Chapter 7
Performing Administrative Functions

You access many of the administrative functions discussed in this chapter from the Site Manager Administration menu. For general information about using the Site Manager Administration menu, see "Performing Administrative Functions" in Chapter 1. For specific information about using buttons, windows, and other Site Manager features, refer to *Using Site Manager Software*.

This chapter describes how to

- Boot a router
- Clear the event log
- Set a router's date and time
- Ping a remote device
- Reallocate memory partitions for a processor module

Router Booting Procedures

Booting a router warm-starts every processor module in the router. Pressing the Reset button on the front panel of the router performs the same procedure.

Note: *You can use Site Manager to warm-start a router only. To cold-start a router to initiate diagnostic tests, you must physically power off and then power on the router, or use the* **diags** *command from the Technician Interface. Refer to* Using Technician Interface Software *for more information.*

You must boot a router to use a new configuration file or router software image.

FN/LN/CN Router Boot Prerequisite

The PCMCIA/Floppy switch on the Flash System Controller board of an FN™, LN®, or CN® determines where the router looks for the image (*ace.out*) and configuration file when it is booting. The PCMCIA (Personal Computer Memory Card International Association) position is for memory card boot access, and the Floppy position is for diskette boot access.

You can use Site Manager and the Technician Interface to access both the memory card and diskette files, regardless of the position of this switch. But you cannot override the switch setting when booting. For example, you cannot boot from a diskette if the switch is set in the PCMCIA position.

When you use the Site Manager to boot the router, or to specify an image and configuration file in a Technician Interface **boot** command, the software verifies the file's existence before allowing the boot to take place.

If the PCMCIA/Floppy switch is in the PCMCIA setting and you boot the router, the following occurs:

1. The router boots from *1:ace.out* if it is available. If not, it boots from *2:ace.out* if it is available. If both are unavailable, a boot error occurs.
2. The router configures from *1:config* if it is available. If not, it configures from *2:config* if it is available. If both are unavailable, a configuration error occurs.

Booting a Router

To boot a Bay Networks router, start from the Site Manager main window and follow these steps:

1. **Select Administration→Boot Router.**

   The Boot Router window shows default filenames for the router software image and the configuration file (Figure 7-1).

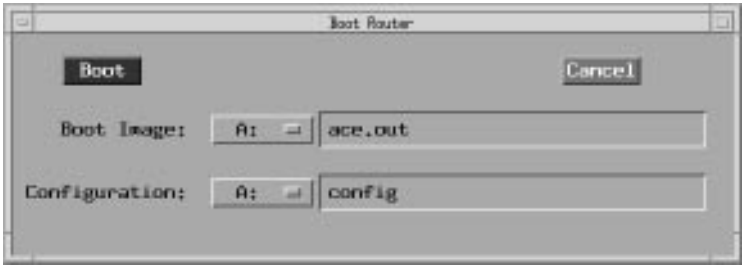

Figure 7-1. Boot Router Window

You can enter alternative filenames in this window. The Boot Router window also shows two default router volumes for the router software image and configuration file. You can select alternative volumes as well.

2. **To boot from a router software image other than the one displayed, enter an image filename in the Boot Image field.**
3. **Select the rectangle next to the Boot Image volume.**

   A popup window shows the available router volumes.
4. **Select the volume where the image specified in Step 2 is located.**

   The popup window closes and the new volume is displayed.
5. **To boot from an alternative configuration file, enter a configuration filename in the Configuration field.**
6. **Select the rectangle next to the Configuration volume shown.**

   A popup window shows the available router volumes.
7. **Select the volume where the configuration file specified in Step 5 is located.**

   The popup window closes and the new volume appears.
8. **Click on Boot.**

   A confirmation window appears.
9. **Click on OK.**

   Wait a few minutes to give the router time to reboot.

10. **To determine if the router booted correctly, select View→Refresh Display from the main Site Manager window.**

If the router booted correctly, system information appears in the main Site Manager window.

The same defaults appear in the Boot Router window after every boot. Depending on the router, the following may appear:

- The name of the router's boot image (the section "Default Filenames" in Chapter 5 lists the names of the boot images for the different Bay Networks routers)
- *config* for all routers
- Volume number for routers using a memory card or Single Inline Memory Module (SIMM)
- Volume indicated by the letter A for routers using a diskette

Using Delayed Boot

Delayed Boot, or Remote User Interface Boot (RUI Boot), lets you specify the exact date and time a Bay Networks router boot takes place. It functions in all other aspects as a normal boot initiated from the Administration menu of Site Manager. To perform a normal boot, see "Booting a Router," in the previous section.

You schedule a Delayed Boot using the Configuration Manager available from the Tools menu of Site Manager. For more information on the Configuration Manager, refer to *Configuring Routers* or *Configuring Customer Access and Trunks (BNX Software)*.

This section describes how to

- Enable and disable the Delayed Boot feature
- Schedule one or more Delayed Boots
- Modify a scheduled Delayed Boot
- Delete a scheduled Delayed Boot

Enabling and Disabling Delayed Boot

You can globally enable or disable the Delayed Boot feature. When you enable Delayed Boot, you can schedule a router for a Delayed Boot. When you disable Delayed Boot, you can continue to schedule router boots; however, no boots will occur until you re-enable the feature.

Note: *Disabling Delayed Boot does not alter the boot schedule. If Delayed Boot is later enabled, any routers whose boot time has not expired will boot as scheduled.*

To enable and disable Delayed Boot, start at the Configuration Manager and complete the following steps:

1. **Select Platform→Schedule Boot→Global.**

   The RUI Boot Group List window appears (Figure 7-2).

Figure 7-2. RUI Boot Group List Window

2. **Edit the parameter.**
   - — Enter Enable to globally enable Delayed Boot.
   - — Enter Disable to globally disable Delayed Boot.
3. **Click on OK to return to the Configuration Manager main window.**

Scheduling a Delayed Boot

Delayed Boot lets you specify the exact date and time a router boot occurs, and the image and configuration file the router will use.

To schedule a Delayed Boot of a Bay Networks router, start at the Configuration Manager and complete the following steps:

1. **Select Platform→Scheduled Boot→Boot.**

   The RUI Boot Interface Parameters window appears (Figure 7-3).

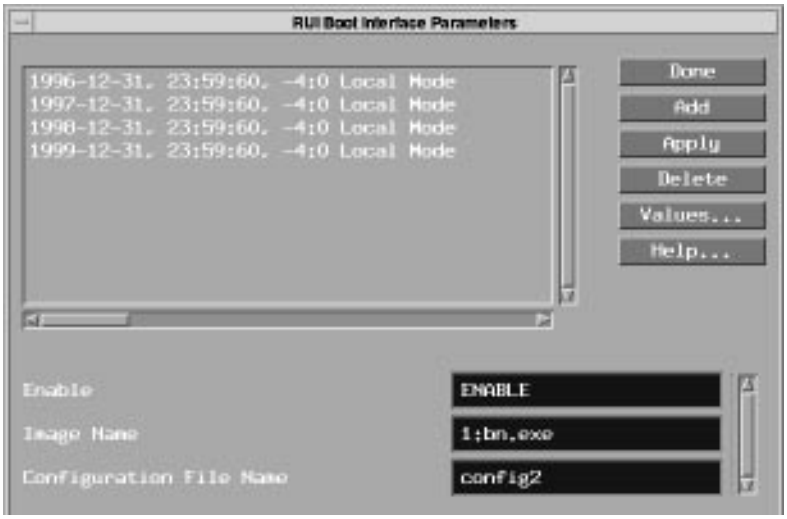

Figure 7-3. RUI Boot Interface Parameters Window

2. **Click on Add.**

   The RUI Boot Parameters window appears (Figure 7-4).

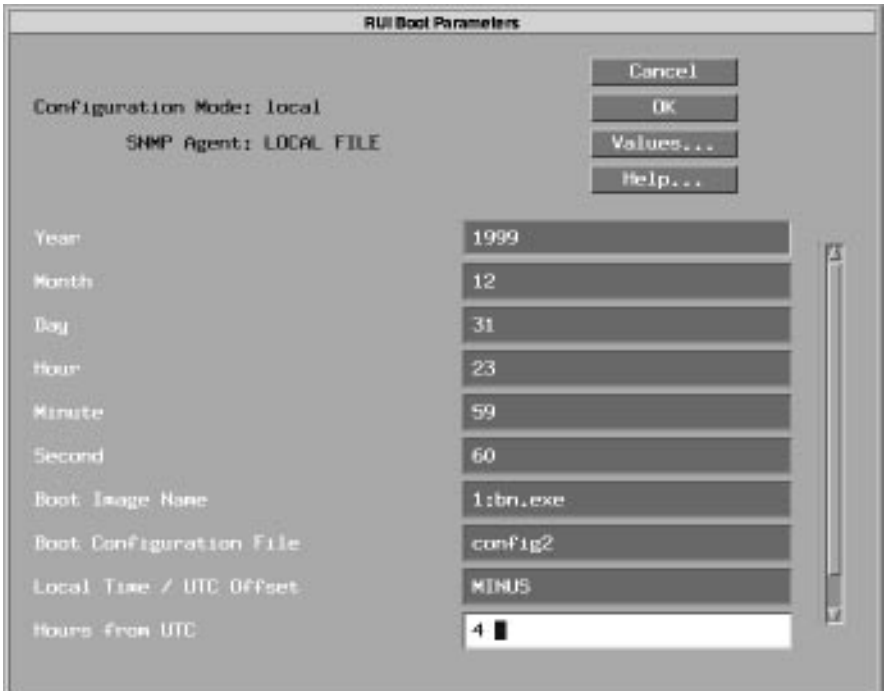

Figure 7-4. RUI Boot Parameters Window

3. **Enter the appropriate information in each of the active fields.**

   You must complete all the active fields to schedule a Delayed Boot. Refer to Table 7-1 for the field names and the range of acceptable values.

Caution: *For a Delayed Boot to occur, you must enter PLUS or MINUS and the appropriate Universal Time Code (UTC) Offset in the Local Time/UTC Offset field. You cannot enter LOCAL unless the Gmt offset of the scheduled router's system clock is set to zero.*

The values you enter in the Local Time/UTC Offset field must be uppercase (as shown in Table 7-1). Once you enter PLUS or MINUS, the fields Hours from UTC and Minutes from UTC become active (use the scroll bar to access the Minutes from UTC field). Enter the appropriate information and proceed to the next step.

4. **Click on OK.**

   You will see the RUI Boot Interface Parameters window with the image name and configuration file of the appropriate router. The date and time of the Delayed Boot appears in the upper-left corner. All scheduled Delayed Boots are listed here.

5. **Click on Done to return to the Configuration Manager main window.**

   A Delayed Boot is now scheduled and will automatically occur on the routers you selected, at the date and time you selected, using the boot image and configuration file you selected.

Table 7-1. Delayed Boot Parameter Fields and Acceptable Values

Field	Range
Year	1970 - 2070
Month	1 - 12
Day	1 - 31
Hour	0 - 23
Minute	0 - 59
Second	0 - 60
Boot Image File	Any valid boot image
Boot Configuration File	Any valid Configuration file
Local Time/Universal Time Code (UTC) Offset	LOCAL, PLUS, MINUS*
Hours from UTC	0 - 11
Minutes from UTC	0 - 59

*. The values you enter in the Local Time/UTC Offset field must be uppercase.

Modifying a Scheduled Delayed Boot

Note: *To modify the date and time of a Delayed Boot, you must cancel and re-schedule the boot. Refer to the section "Deleting a Scheduled Delayed Boot," later in this chapter.*

To modify a Delayed Boot on a particular router, you edit the Enable, Image Name, and Configuration File Name parameters. Start at the Configuration Manager and complete the following steps:

1. **Select Platform→Scheduled Boot→Boot.**

   The RUI Boot Interface Parameters window appears (refer to Figure 7-3).

2. **From the list in the upper-left corner of the window, select the Delayed Boot you want to modify.**

3. **Edit the Enable, Image Name, or Configuration File Name field.**

   Refer to Table 7-1 for the field names and the range of acceptable values.

4. **Click on Apply.**

   The Delayed Boot of the router you selected is modified.

5. **Select Done to return to the Configuration Manager main window.**

Deleting a Scheduled Delayed Boot

Note: *To modify the date and time of a Delayed Boot, you must cancel and re-schedule the boot. Complete the steps below and refer to the section "Scheduling a Delayed Boot," earlier in this chapter.*

To modify the Enable, Image Name, and Configuration File Name parameters of a Delayed Boot, refer to the previous section, "Modifying a Scheduled Delayed Boot."

You can delete one or all scheduled Delayed Boots. To delete all scheduled Delayed Boots, proceed to the next section. To delete a Delayed Boot on a particular router, start at the Configuration Manager and complete the following steps:

1. **Select Platform→Scheduled Boot→Boot.**

   The RUI Boot Interface Parameters window appears (refer to Figure 7-3).

2. **From the list in the upper-left corner of the window, select the scheduled RUI Boot you want to cancel.**
3. **Click on Delete.**

   The scheduled Delayed Boot is deleted.
4. **Click on Done to return to the Configuration Manager main window.**

Deleting All Scheduled Delayed Boots

You can delete all scheduled Delayed Boots from the current version of Site Manager. If you delete all scheduled Delayed Boots, you cannot recover them.

Note: *To disable all scheduled Delayed Boots without deleting them, refer to the section "Enabling and Disabling Delayed Boot."*

To delete all scheduled Delayed Boots, start at the Configuration Manager and complete the following steps:

1. **Select Platform→Schedule Boot→Delete.**

   The Delete RUI Boot message window appears (Figure 7-5).

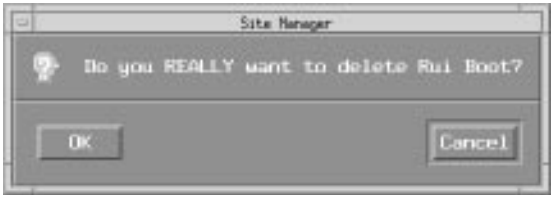

Figure 7-5. Delete RUI Boot Message Window

2. **Select OK.**

   You have deleted all scheduled Delayed Boots from the current version of Site Manager.

Specifying Values for Delayed Boot Parameters

Use the information in this section to specify values for Delayed Boot (RUI Boot) parameters. For each parameter, this section provides information about default settings, valid parameter options, the parameter function, instructions for setting the parameter, and the Management Information Base (MIB) object ID.

The Technician Interface lets you modify parameters by issuing **set** and **commit** commands that specify the MIB object ID. This process is equivalent to modifying parameters using Site Manager.

For more information about using the Technician Interface to access the MIB, refer to *Using the Technician Interface Software*.

Caution: *The Technician Interface does not verify that the value you enter for a parameter is valid. Entering an invalid value can corrupt your configuration.*

Parameter:	**Disable**
Default:	Enable
Options:	Enable | Disable
Function:	Enables or disables Delayed Boot on all the routers you have scheduled to boot.
Instructions:	Select Disable to prevent routers you have scheduled for Delayed Boot from booting. Select Enable to allow routers you have scheduled for Delayed Boot to boot.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.14.1.2

Parameter:	**Delete**
Default:	Created
Options:	Delete
Function:	Cancels a Delayed Boot of a particular router.
Instructions:	Select Delete to cancel a Delayed Boot on a particular router from occurring.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.14.2.1.1

Parameter: **Disable**

Default: Enable

Options: Enable | Disable

Function: Enables or disables a scheduled Delayed Boot of a particular router.

Instructions: Select Enable to allow a Delayed Boot of a particular router to occur as scheduled. Select Disable to prevent a Delayed Boot of a particular router from occurring.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.14.2.1.2

Parameter: **Date and Time**

Default: None

Range: Year, Month, Day, Hour, Minute, Second, Local Time/Universal Time Code (UTC) Offset, Hours from UTC

Function: Determines the date and time that a Delayed Boot is scheduled to occur. Refer to Table 7-2 for the field names and a range of acceptable values.

Table 7-2. Delayed Boot Fields and Values

Field	Range
Year	1970 - 2070
Month	1 - 12
Day	1 - 31
Hour	0 - 23
Minutes	0 - 59
Seconds	0 - 60
Local Time/UTC Offset	LOCAL, PLUS, MINUS*
Hours from UTC	0 - 11
Minutes from UTC	0 - 59

*. The values you enter in the Local Time/UTC Offset field must be uppercase.

Instructions: Enter the date and time you want the Delayed Boot to occur.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.14.2.1.4

Parameter:	**Boot Image Name**
Default:	None
Options:	Any valid boot image.
Function:	Determines the router boot image.
Instructions:	Enter the boot image name you want the router scheduled for Delayed Boot to use.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.14.2.1.5

Parameter:	**Boot Configuration File**
Default:	None
Options:	Any valid configuration file.
Function:	Determines the router configuration file.
Instructions:	Enter the configuration file you want the router scheduled for Delayed Boot to use.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.14.2.1.6

Booting a Processor Module

Booting a processor module by using the Reset Slot option warm-starts a single processor module in the router.

The reset option allows you to reboot a processor module with the boot image and configuration file the router is currently using.

You may want to reset a slot to troubleshoot a problem you are having with a router. To reset a slot, follow these directions:

1. **From the main Site Manager window, select Administration→Reset Slot.**

   The Reset Slot window appears (Figure 7-6), showing the router's default slot.

Figure 7-6. Reset Slot Window

2. **Click the rectangle adjacent to the slot number.**

   A popup window shows the available slots (Figure 7-7).

Figure 7-7. Selecting a Slot

3. **Select the slot where you want to boot a processor module.**

   The popup window closes and the slot number you selected appears.

4. **Click on Reset.**

   A confirmation window appears.

5. **Click on OK.**

When you boot a processor module (reset a slot), the following occurs:

1. The operating router software running on the processor module forwards a boot request to the other processor modules.
2. The first processor module to respond to the boot request forwards the boot image resident in its memory.

3. The resetting processor module receives and executes the boot image. At this instant, the router disrupts connectivity to the associated slot and to the services provided in that slot. The other processor modules resynchronize their routing tables after the slot fails to receive packets.
4. The resetting processor module completes the boot process and requests a configuration. The first available processor module forwards the configuration resident in its memory.
5. The resetting processor module loads the configuration image and initiates the services provided by the slot, thus re-establishing connectivity. The resetting processor module alerts the other processor modules that it can receive packets.
6. The other processor modules resynchronize their routing tables accordingly.

Clearing the Event Log

To clear a router's current event log, follow these steps:

1. **Select Administration→Clear Event Log.**

   A confirmation window appears.

2. **Click on OK to delete all the event messages currently stored in the router's memory.**

   New event messages automatically start filling the event log again.

Setting a Router's Date and Time

You can use the Router Date and Time command to update the router's date, time, and time zone.

To set the time and date recorded on the router, follow these steps:

1. **From the main Site Manager window, select Administration→Router Date and Time.**

   The Router Date and Time window appears (Figure 7-8).

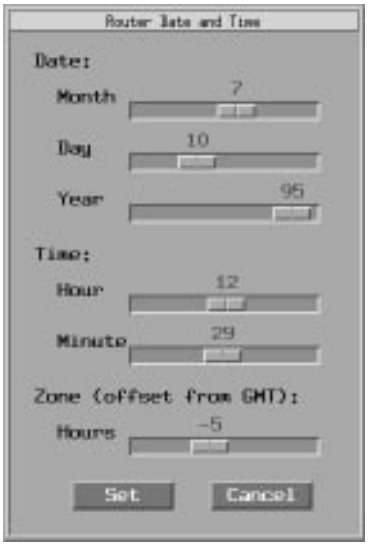

Figure 7-8. Router Date and Time Window

2. **Use the slidebar in each field to specify the correct information. Then click on Set.**

   The Zone field lets you specify the number of hours your time zone is ahead of or behind Greenwich mean time (GMT). Move the slidebar to the left to select a value behind (-) GMT. Move the slidebar to the right to select a value ahead of GMT. For example, Eastern Standard Time Zone is 5 hours behind GMT, so you would select -5.

Pinging a Remote Device

The Ping from Router option lets you test the reachability of a remote device using one of the following protocols: IP, IPX, OSI, VINES, AppleTalk, and APPN.

You ping from the router by selecting Administration→Ping from Router and then one of the protocols listed in the menu (Figure 7-9).

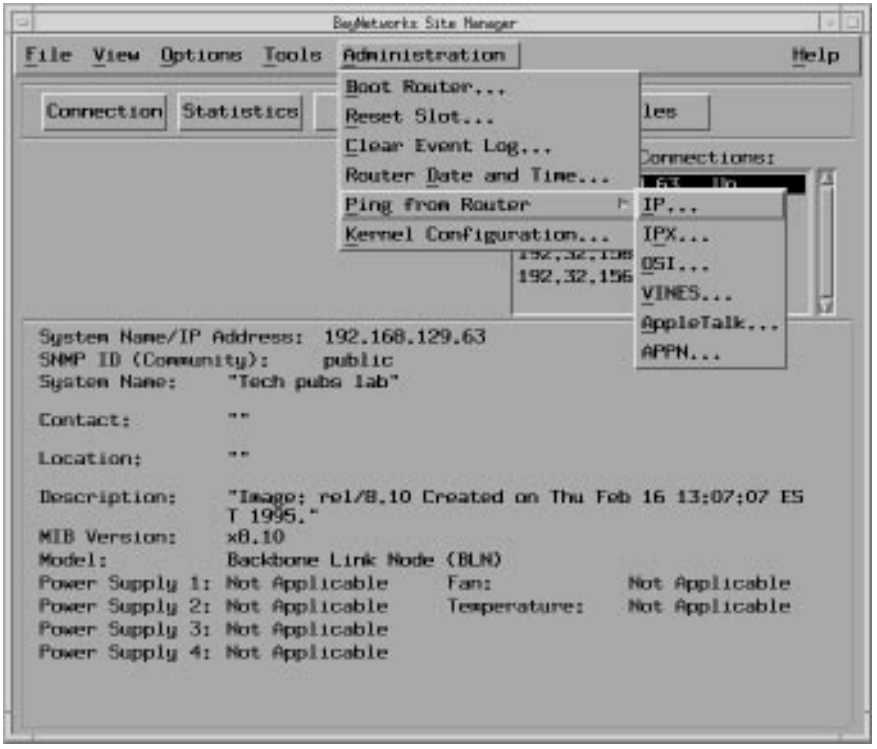

Figure 7-9. Selecting Ping from Router Option

The following sections describe the available ping options.

IP Ping

When you ping a remote device using the Internet Protocol, the ping program residing on the router sends an Internet Control Message Protocol (ICMP) echo request to the remote address you specified in the IP Ping window. The remote device responds to the router's request if it is reachable. A message window pops up, showing the response or the result of the request.

To send an ICMP echo request to a remote device running IP, proceed as follows:

1. **Select Administration→Ping from Router→IP.**

   The IP Ping window appears (Figure 7-10).

Figure 7-10. IP Ping Window

2. **In the IP Address field, enter the IP address of the remote device, in dotted decimal notation.**
3. **In the Timeout field, enter the number of seconds after which you want each ping to time out. The default Timeout is 1 second.**

   If the router receives a response to a ping after the ping has timed out, it does not send an "alive" message to Site Manager.
4. **In the Retries field, enter the number of successive times the router should repeat the ping. The default for Retries is 0.**

   The router does not wait for the timeout before it sends the next ping.
5. **In the Packet Size field, enter the number of bytes of data to send with each ping. The default Packet Size is 16.**
6. **In the Traceroute field, specify y (yes) if you want the router to generate a path report that shows the intervening hop addresses to the destination. The default for Traceroute is n (no).**
7. **Click on Ping.**

IP Ping Responses

Site Manager displays one of the following messages when you click on Ping. (If you enter a value other than 0 for Retries, Site Manager displays one of the following messages for the default ping, plus one for each additional ping.)

- An “alive” message appears if the router received an ICMP echo response from the target device within the timeout allowed. The message also provides the size of the test packet. Figure 7-11 shows a sample message.

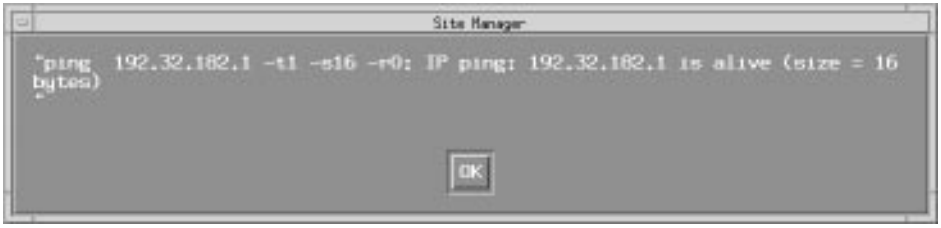

Figure 7-11. Ping Is Alive Window

- A “does not respond” message appears if the media access control (MAC) address of the target device is resolved, but the router did not receive an ICMP echo response from the target device within the timeout allowed. Figure 7-12 shows a sample message.

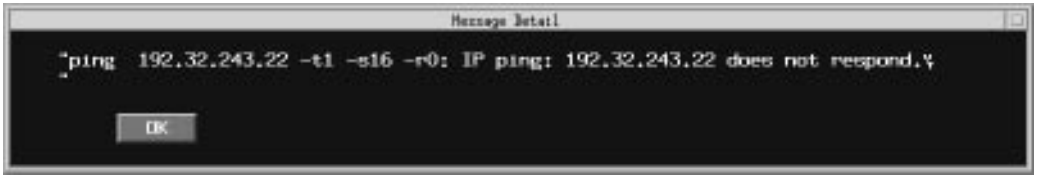

Figure 7-12. Ping Does Not Respond Window

- An “ICMP host unreachable from <y.y.y.y>” message appears if the router whose address is *y.y.y.y* cannot forward the ping request any further along the path to the target device. IP updates its IP routing or Address Resolution Protocol (ARP) table accordingly. A sample message follows:

  ```
  ping: ICMP host unreachable from 192.32.243.1
  ```

- A target address “is unreachable” message appears if the router previously issued an “ICMP host unreachable from <y.y.y.y>” message. Within 40 seconds, the router receives a subsequent ICMP echo request addressed to the same target device. The ARP times out or the address is not resolved. A sample message follows:

  ```
  ping: 192.32.1.151 is unreachable
  ```

IPX Ping

When you issue an Internet Packet Exchange Protocol (IPX) ping, the router sends an IPX configuration request packet to the remote IPX address that you specify. If the remote device is listening on socket number 456h for an IPX configuration request packet, it responds if it can be reached, and Site Manager displays a message indicating that the device “is alive” or “does not respond.”

IPX configuration request packets are typically used to get configuration information from other devices on a NetWare network. However, the router only uses these packets to test the reachability of a remote device that listens for and responds to IPX configuration request packets.

The IPX router will not send or acknowledge IPX configuration request packets addressed to

- Network 0x00000000 (local network destination) or network 0xFFFFFFFF
- Host 0x000000000000 or host 0xFFFFFFFFFFFF (broadcast host destination)

The IPX router will only respond to request packets sent directly to one of its interface addresses. If you send a request packet from a router to an IPX interface on that same router, the router does not send the request packet out onto the line. Instead, the router sends the packet internally to the specified interface, which then responds internally.

Note: *The IPX router will respond (reply with a ping response) to any ping packet that comes in on socket number 9086 and that has a type field of 0.*

To send an IPX configuration request packet, proceed as follows:

1. **Select Administration→Ping from Router→IPX.**

   The IPX Ping window appears (Figure 7-13).

Figure 7-13. IPX Ping Window

2. **In the Address field, enter the IPX address of the remote device, in hexadecimal or decimal notation.**

   An IPX address consists of a 4-byte network address and a 6-byte host address, separated by a period (for example, 0x0000AB12.0x000000CD1234 [leading zero padding is not required]). 0x indicates that the address is in hexadecimal notation.

   An IPX address in decimal notation consists of a 4-byte network address and a 6-byte host address, where each byte is a number between 0 and 255, inclusive, and each byte is separated from the next byte by a period (for example, 0.1.23.47.0.0.0.1.2.55).

Note: *If you issue an IPX ping to an entity on a Token Ring network, you must enter the host portion of the IPX address in byte-swapped (noncanonical) form.*

3. **In the Timeout field, enter the number of seconds after which each ping times out. The default Timeout is 1 second.**

   If the router receives a response to a ping after it times out, it does not send an "alive" message to Site Manager.

4. **In the Retries field, enter the number of successive times the router should repeat the ping. The default for Retries is 0.**

   The router does not wait for the timeout before sending the next ping.

5. **Click on Ping.**

IPX Ping Responses

Site Manager displays one of the following messages when you issue an IPX ping. (If you enter a value other than 0 for Retries, Site Manager displays one of the following messages for the default ping, plus one for each additional ping.)

- A target address “is unreachable” message appears if the router cannot find the specified network address in its table of IPX networks. A sample message follows:

  ```
  IPX ping:  0xAB12.CD1234 is unreachable
  ```

- An “alive” message appears if the router receives an IPX reply packet from the target device within the timeout allowed. A sample message follows:

  ```
  IPX ping:  0xAB12.CD1234 is alive
  ```

- A “does not respond” message appears if the IPX address of the target device is resolved, but the router does not receive an IPX reply packet from the target device within the timeout allowed. A sample message follows:

  ```
  IPX ping:  0xAB12.CD1234 does not respond
  ```

- An “invalid parameter specified” message appears if the network or host address is all 0s, all Fs, or not a valid IPX address. A sample message follows:

  ```
  IPX ping:  invalid parameter specified
  ```

- A “resource error” message appears if the router cannot allocate a buffer for the request because no buffers are available. A sample message follows:

  ```
  IPX ping: resource error
  ```

OSI Ping

When you issue an Open Systems Interconnection (OSI) ping, the router sends a Connectionless Network Protocol (CLNP) echo request to the remote network service access point (NSAP) address you specify. The remote device responds if it can be reached, and Site Manager displays the response or the result of the request.

To send a CLNP echo request, proceed as follows:

1. **Select Administration→Ping from Router→OSI.**

   The OSI Ping window appears (Figure 7-14).

Figure 7-14. OSI Ping Window

2. **In the Address field, enter the NSAP address of the remote device, in hexadecimal notation.**
3. **In the Timeout field, enter the number of seconds the router should wait for a response from the remote device. The default Timeout is 1 second.**
4. **In the Retries field, enter the number of successive times the router should repeat the ping.**

   The router does not wait for the timeout before it sends the next ping after a response to a previous ping is received. The default for Retries is 0.
5. **Click on Ping.**

OSI Ping Responses

Site Manager displays one of the following messages when you issue an OSI ping. (If you enter a value other than 0 for Retries, Site Manager displays one of the following messages for the default ping plus one for each additional ping.)

- An “alive” message appears if the router receives a CLNP echo response from the target device within the timeout allowed. A sample message follows:

  ```
  OSI ping: 49000400000a12121200 is alive
  ```
- A target address “is unreachable” message appears if the local router cannot find the specified address in its routing table. A sample message follows:

  ```
  OSI ping: 49000400000a12121200 is unreachable
  ```

- A “does not respond” message appears if the NSAP address of the target device is resolved, but the router does not receive a CLNP echo response from the target device within the timeout allowed. A sample message follows:

  ```
  OSI ping: 49000400000a12121200 does not respond
  ```

- An “NSAP address is too short” message appears if the NSAP address is too short. The minimum allowed NSAP address length is 20 hexadecimal characters (10 bytes). A sample message follows:

  ```
  OSI ping: NSAP address is too short
  ```

- An “OSI service is not running” message appears if the OSI service is not enabled on the router. A sample message follows:

  ```
  OSI ping: OSI service is not running
  ```

- A “resource error” message appears if the router cannot allocate a buffer for the request because no buffers are available. A sample message follows:

  ```
  OSI ping: resource error
  ```

- A “system error” message appears if the Technician Interface has failed. A sample message follows:

  ```
  OSI ping: system error
  ```

- A “<y.y.y.y.y.y.y.y.y.y.y.y.y.y.y.y.y.y.y.y> is a bad NSAP address” message appears if the NSAP address is more than 20 hexadecimal characters or nonhexadecimal characters.

  y.y.y.y.y.y.y.y.y.y.y.y.y.y.y.y.y.y.y.y is the address of the CLNP host.

  A sample message follows.

  ```
  OSI ping: 123456Z  is a bad NSAP address
  ```

VINES Ping

When you issue a VINES ping to a remote VINES device, the router responds if the device can be reached, and Site Manager displays the response or the result of the request.

To send a VINES request to determine the network connectivity of a VINES host, proceed as follows:

1. **Select Administration→Ping from Router→VINES.**

   The VINES Ping window appears (Figure 7-15).

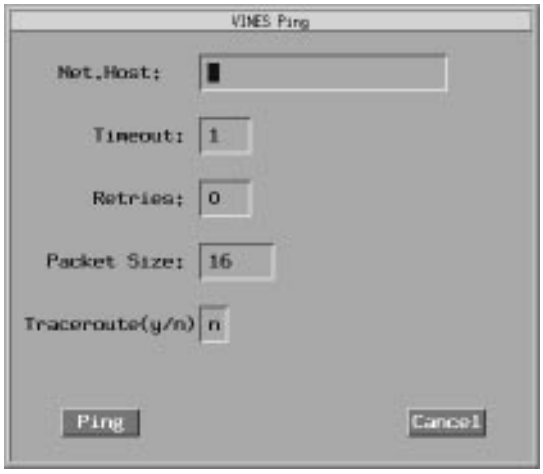

Figure 7-15. VINES Ping Window

2. **In the Network Host field, enter the network and host address of the remote device you want to ping.**

   The Network ID is the 32-bit serial number of the server node that identifies the logical grouping of nodes on a VINES network. The Host address is the 16-bit subnetwork number that identifies the node within the server node's logical grouping.

Note: *You can enter the network and host addresses in decimal or hexadecimal format. If you use hexadecimal format, precede each address with the 0x prefix.*

3. **In the Timeout field, enter the number of seconds after which each ping times out. The default Timeout is 1 second.**

   If the router receives a response to a ping after it has timed out, it does not send an "alive" message to Site Manager.

4. **In the Retries field, enter the number of successive times the router should repeat the ping. The default for Retries is 0.**

   The router does not wait for the timeout before it sends the next ping.

5. **In the Packet Size field, enter the number of bytes of data to send with each ping. The default is 16.**

6. **In the Traceroute field, specify y (yes) if you want the router to generate a path report that displays the intervening hop addresses to the destination. The default is n (no).**
7. **Click on Ping.**

VINES Ping Responses

Site Manager displays one of the following messages when you issue a VINES ping (if you enter a value for Retries, Site Manager displays one of the following messages for the default ping, plus one for each additional ping):

- An “alive” message appears if the router receives a response from the target device within the timeout allowed. The message also indicates the size of the test packet. A sample message follows:

  ```
  VINES ping: 2705682.8003 is alive (size = 16 bytes)
  ```

- A “does not respond” message appears if the address of the target device is resolved, but the system did not receive a response from the target device within the timeout allowed. A sample message follows:

  ```
  VINES ping: 2705682.8003 does not respond
  ```

- A target address “is unreachable” message appears if the router cannot find the specified address in its routing table. A sample message follows:

  ```
  VINES ping: 2705682.8003 is unreachable
  ```

- A “resource error” message appears if the router cannot allocate a buffer for the request because no buffers are available. A sample message follows:

  ```
  VINES ping: resource error
  ```

- An “invalid parameter specified” message appears if you specify an invalid parameter when you issue a VINES ping. A sample message follows:

  ```
  VINES ping: invalid parameter specified
  ```

- A “VINES service is not running” message appears if the VINES service is not enabled on the router. A sample message follows:

  ```
  VINES ping: VINES service is not running
  ```

AppleTalk Ping

When you issue an AppleTalk ping to a remote AppleTalk device, the router responds if the device can be reached, and Site Manager displays the response or the result of the request.

To send an AppleTalk request to determine the network connectivity of an Appletalk host, proceed as follows:

1. **Select Administration→Ping from Router→AppleTalk.**

   The AppleTalk Ping window appears (Figure 7-16).

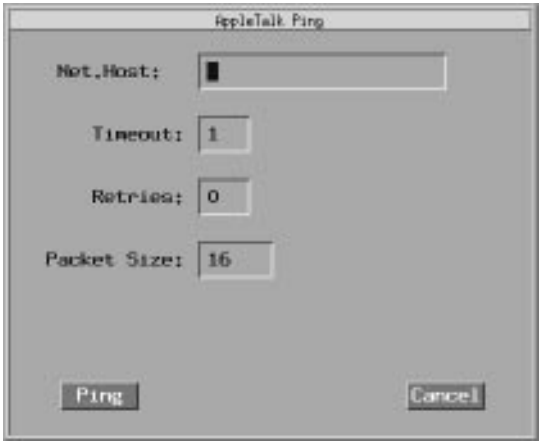

Figure 7-16. AppleTalk Ping Window

2. **In the Net.Host field, enter the network address and node ID of the remote device you want to ping.**

   The range of valid values for an AppleTalk network address is from 1 to 65279 (decimal). The range of valid values for an AppleTalk node ID is from 1 to 254 (decimal).

Note: *You can enter the network address and node ID in decimal or hexadecimal format. (If you use hexadecimal format, precede each address or node ID with the 0x prefix.)*

3. **In the Timeout field, enter the number of seconds after which each ping times out. The default Timeout is 1 second.**

If the router receives a response to a ping after it has timed out, it does not send an "alive" message to Site Manager.

4. **In the Retries field, enter the number of successive times the router should repeat the ping. The default for Retries is 0.**

   The router does not wait for the timeout before it sends the next ping.

5. **In the Packet Size field, enter the number of bytes of data to send with each ping. The default is 16 bytes, and the maximum is 585 bytes.**

6. **Click on Ping.**

AppleTalk Ping Responses

Site Manager displays one of the following messages when you issue an AppleTalk ping (if you enter a value for Retries, Site Manager displays one of the following messages for the default ping, plus one for each additional ping):

- An "alive" message appears if the router receives a response from the target device within the timeout allowed. The message also indicates the size of the test packet. A sample message follows:

  ```
  AppleTalk ping: 2553.217 is alive (size = 16 bytes)
  ```

- A "does not respond" message appears if the address of the target device is resolved, but the system did not receive a response from the target device within the timeout allowed. A sample message follows:

  ```
  AppleTalk ping: 2553.217 does not respond
  ```

- A target address "is unreachable" message appears if the router cannot find the specified address in its routing table. A sample message follows:

  ```
  AppleTalk ping: 2553.217 is unreachable
  ```

- A "resource error" message appears if the router cannot allocate a buffer for the request because no buffers are available. A sample message follows:

  ```
  AppleTalk ping: resource error
  ```

- An "invalid parameter specified" message appears if you specify an invalid parameter when you issue an AppleTalk ping. A sample message follows:

  ```
  AppleTalk ping: invalid parameter specified
  ```

- An "AppleTalk service is not running" message appears if the AppleTalk service is not enabled on the router. A sample message follows:

  ```
  AppleTalk ping: Appletalk service is not running
  ```

APPN Ping

When you issue an APPN ping to a remote APPN device, the remote device responds if it can be reached, and Site Manager displays the response or the result of the request. APPN ping uses the APING (APPN Ping) Transaction Program (TP) to send an APING request to the APINGD TP running on the remote device.

To send an APPN ping request, proceed as follows:

1. **Select Administration→Ping from Router→APPN.**

   The APPN Ping window appears (Figure 7-17).

Figure 7-17. APPN Ping Window

2. **In the Target CP/LU Name field, enter the required APPN address, in the format of a Control Point name, of the remote device. Use the format *<network ID>.<CP name>* if the remote device is not on the same network as the system from which you are pinging.**

3. **In the Mode Name field, optionally enter one of the following values:**

   — #INTER for interactive mode, for example, when there is not much data involved and response time is very important.

   — #BATCH for batch-like mode, when there is a lot of data involved and response time is not important.

   — #INTERSC for a secure version of interactive mode.

   — #BATCHSC for a secure version of the batch-like mode.

   You can leave this field blank to use the default mode, which is similar to #INTER.

   APPN route calculation uses the mode characteristics when determining the optional route. Specifying a mode for the ping will test whether a route exists that is suitable to carry the type of traffic that the mode identifies.

4. **In the Data Size field, enter the number of bytes of data to send with each ping. The default is 100.**

5. **In the Retries field, enter the number of successive times the router should repeat the ping. The default for Retries is 1.**

   The router does not wait for the timeout before it sends the next ping.

6. **In the Timeout field, enter the number of seconds after which each ping times out. The default Timeout is 15 seconds.**

   If the router receives a response to a ping after it has timed out, it does not send an “alive” message to Site Manager.

7. **Click on Ping.**

APPN Ping Responses

Site Manager displays one of the following messages when you issue an APPN ping; Site Manager displays only one message, regardless of the number of retries you specified:

- An alive message appears if the router receives a response from the target device within the timeout allowed. A sample message follows:

  ```
  APPN ping: bay is alive
  ```

- A “did not complete in the time allowed” message appears if the node is alive but congested, the data transfer time exceeded the timeout, or the directory search is not complete. A sample message follows:

```
APPN ping: ping of bay did not complete in the time allowed
```

- An “unreachable” message appears if no route could be calculated to the remote device or if the remote device does not support APINGD. A sample message follows:

  ```
  APPN ping: bay is unreachable
  ```

- An “invalid name” message appears if the specified node name or mode name is invalid. A sample message follows:

  ```
  APPN ping: invalid name specified
  ```

- An “APPN service is not running” message appears if the APPN service is not enabled on the router. A sample message follows:

  ```
  APPN ping: APPN service is not running
  ```

Reallocating Memory Partitions for a Processor Module

Using the Site Manager’s Kernel Configuration tool, you can reallocate memory for the following routers and processor modules:

AFN	The AFN router contains a single processor module.
AN	The AN router contains a single processor module.
ASN	The ASN router contains a single processor module.
ACE32 (8MB or greater)	The ACE32 processor module is used in VME-based routers — CN, LN, FN, and ALN.
FRE2	The FRE2 processor module is used in the BLN, BLN-2, and BCN routers.

Partitioning Overview

Processor modules in a router use three types of memory:

- Global memory
- Local memory
- Nonvolatile RAM (NVRAM)

Global and local memory are separate partitions of a single, contiguous memory address space. The RAM chips associated with this address space exist physically on each processor module.

The NVRAM for each processor module stores the memory partitioning configuration associated with that module. You cannot partition NVRAM.

Note carefully the differences in how NVRAM supports processor modules in PPX- and VME-bus Bay Networks routers:

FRE2 (PPX-based routers)	NVRAM is present on each FRE2 processor module inside the router.	If you move a FRE2 module to another slot in the router, the memory partitioning configuration moves with the FRE2 module to the new slot.
ACE32 (VME-based routers)	For routers using ACE32 processor modules, NVRAM is only present on the SYSCON processor module.	If you move an ACE32 module to another slot in the router, the memory partitioning configuration does *not* move with the ACE32 module to the new slot. The partitioning remains in effect at the original slot location.

You can specify the amount of local and global memory (that is, the size of the local and global memory partitions) used by a given processor module. Increasing the size of the Global Memory partition automatically decreases the size of the Local Memory partition. The router software ensures that the sum of local and global memory always equals the total amount of memory available on a given processor.

Site Manager does not allow you to configure more than 4 MB of global memory to an ACE32 processor if an ACE25 module resides in the same router. You overcome this constraint in a router with an ACE32 processor by upgrading any ACE25 processors in the same router to ACE32 processors.

Repartitioning Global and Local Memory

Caution: *You should change memory partitioning only at the recommendation of, or under the direction of, the Bay Networks Technical Response Center. Under normal router and network operating conditions, you should have no need to modify the default memory partitions established for a processor module. You reallocate processor memory partitions in rare instances, and only for the purpose of network troubleshooting.*

To repartition global and local memory, start at the Site Manager main window and follow these steps:

1. **Click on Connection or select Options→Connections.**

   The Router Connection Options window appears (Figure 7-18).

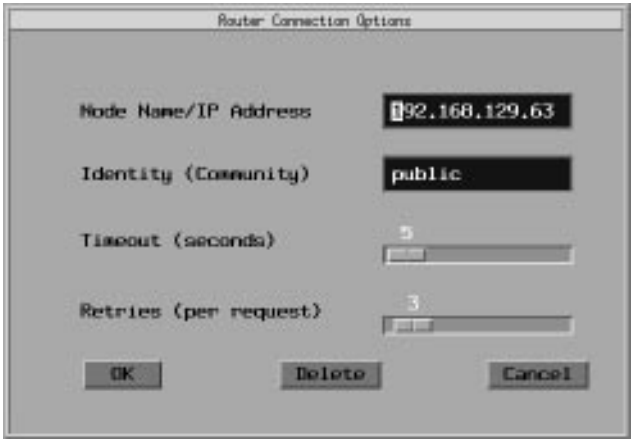

Figure 7-18. Specifying Router Connection Options

2. **Enter the IP address of a router that requires processor memory repartitioning, and set the Timeout and Retry options. Then click on OK.**
3. **From the main Site Manager window, select Administration→Kernel Configuration.**

   The Kernel Configuration window appears (Figure 7-19).

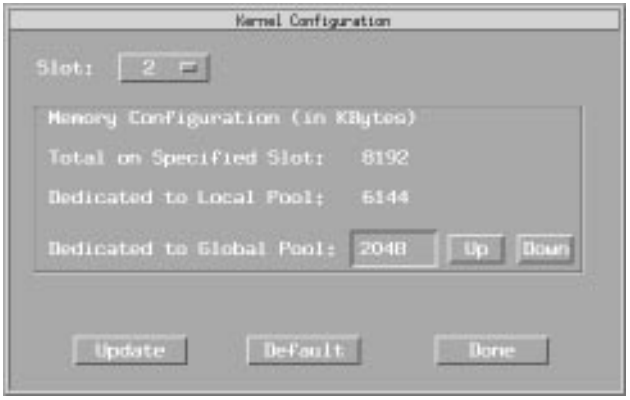

Figure 7-19. Kernel Configuration Window

Note: *If the router you are configuring is not an AN, AFN, or ASN, or if the router does not contain an ACE32 or a FRE2 processor module, a window appears with the following message:*

```
No valid modules were found.
```

The message also means that the processor modules found in the currently connected router are not user-configurable. Such is the case when the Kernel Configuration routine immediately finds only ACE25 or FRE module(s) in the currently connected router.

The Kernel Configuration window displays the following information:

Total memory for the specified slot	Total memory displayed depends on the type of processor module
Memory dedicated to the local pool	Local pool refers to the memory used to manage the router. For example, it contains the statistics, event log, bootable image, and configuration file, along with the routes that IP has learned.
Memory dedicated to the global pool	Global pool refers to the memory dedicated for message buffers.

4. **Select the slot of the processor module that requires memory repartitioning.**

   To do so, click on and hold the Slot button to display all the slots in the router. Then drag the pointer to the desired slot number and release the mouse button.

5. **Enter an amount in the Dedicated to Global Pool field.**

   To add more memory to the global pool, click on Up until the desired amount of memory appears, or type a value in the Dedicated to Global Pool field. As you increase the amount of global memory, you decrease the amount of local memory proportionally.

   To add more memory to the local pool, click on Down until the desired amount of memory appears or type a value in the field.

6. **To restart the slot with the new values, click on Update.**

   A confirmation window prompts

   ```
   Restart slot?
   ```

   (To reset the memory allocation to the factory-default values, click on Default rather than Update. A message then prompts you to confirm your decision to reset the values.)

7. **Click on OK to restart the processor module located in that slot.**

   Site Manager stores the new configuration in NVRAM and restarts the module (ACE32 or FRE2) or router (AN, AFN, or ASN). This store-and-restart process takes about 10 seconds to complete.

8. **Repeat Steps 2 through 7 to reallocate memory partitioning on a different processor module, if applicable.**

Repeat Steps 1 through 7 to reallocate memory partitioning on a processor module in a different router.

9. **When you finish, click on Done in the Kernel Configuration window.**

   The main Site Manager window reappears.

Chapter 8
Using the Ping MIB

For general information about the Ping management information base (MIB), refer to “Tracking Network Availability and Response Time” in Chapter 1. For specific information about using buttons, windows, and other Site Manager features, refer to *Using Site Manager Software*.

To use the Ping MIB to track network availability and response time, you

- Configure IP ping requests
- Review IP ping statistics

Configuring IP Ping Requests

To configure the ping requests for which you want to store the results in the Ping MIB, follow the steps in this section.

Note: *The Ping MIB supports IP ping requests only.*

1. **From the main Site Manager window, click on Connection or select Options→Connections.**

   The Router Connection Options window appears (Figure 8-1).

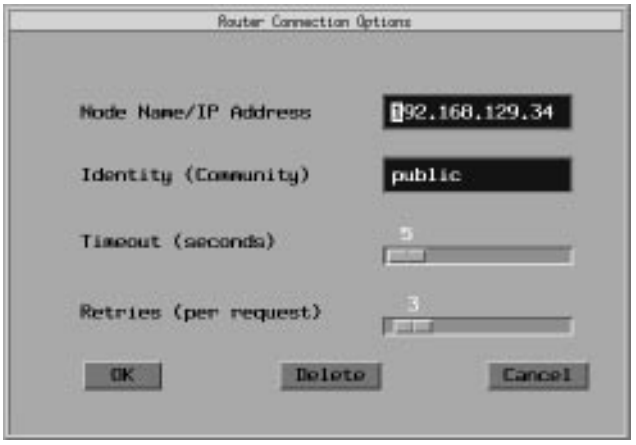

Figure 8-1. Router Connection Options Window

2. **In the Node Name/IP Address field, type the IP address of the router you want to configure. Then click on OK.**

3. **In the main Site Manger window, select Tools→Configuration Manager, and then select the configuration mode you want (Local File, Remote File, or Dynamic).**

   If you choose Local File, the File Selection window appears (Figure 8-2). If you choose Remote File, the Edit Remote Configuration File window appears, and if you choose Dynamic, the Configuration Manager window appears. This chapter assumes you chose the Local File configuration mode. See *Configuring Routers* or *Configuring Customer Access and Trunks (BNX Software)* for information on using the Remote File and Dynamic configuration modes.

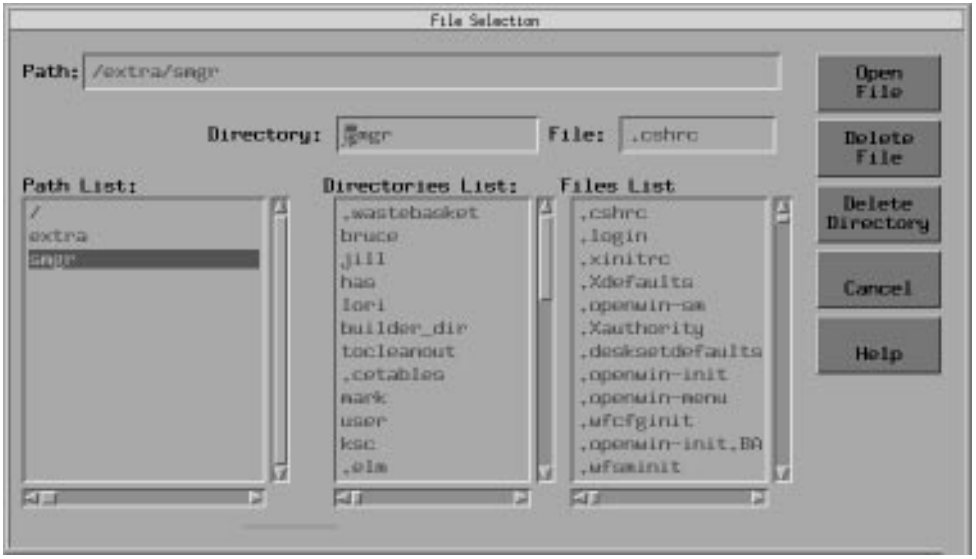

Figure 8-2. File Selection Window

4. **Specify the name of the router's configuration file. Then click on Open File to open the file in the Configuration Manager window (Figure 8-3).**

   For information on how to specify a filename in the File Selection window, see *Configuring Routers* or *Configuring Customer Access and Trunks (BNX Software)*.

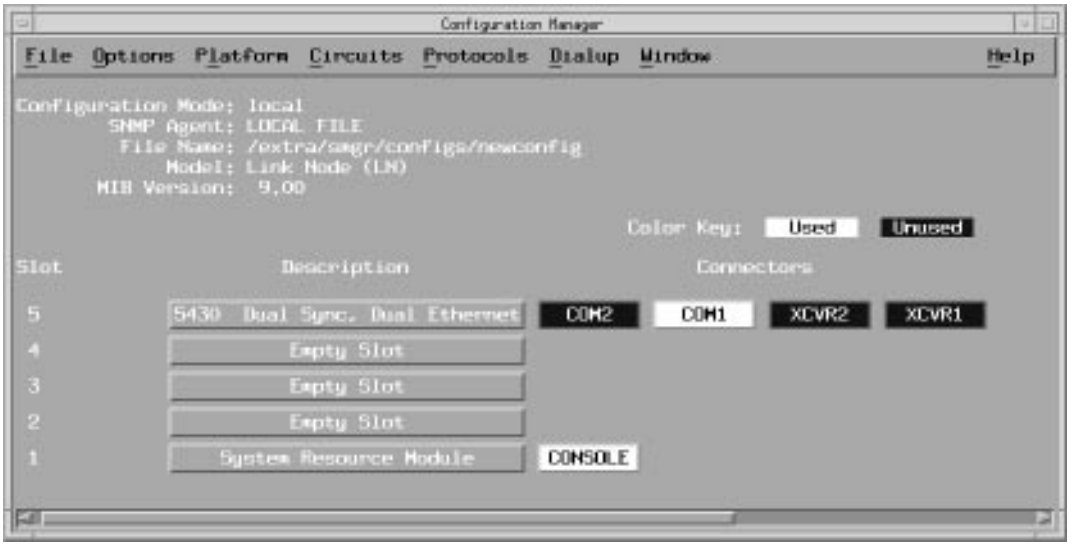

Figure 8-3. Configuration Manager Window

5. **From the Configuration Manager window, select Platform→Ping at Intervals→IP.**

   The Ping at Intervals window appears (Figure 8-4).

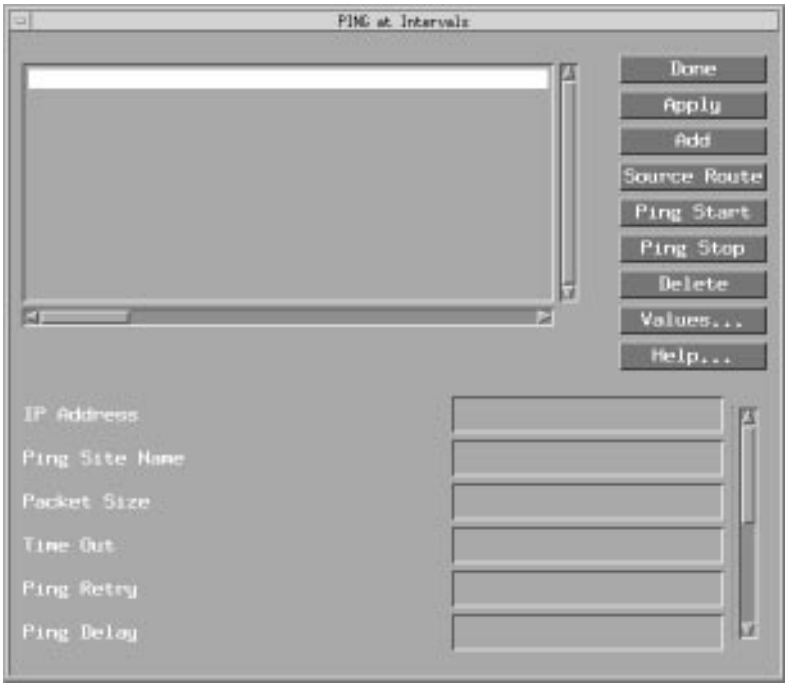

Figure 8-4. Ping at Intervals Window

6. Click on Add.

The IP Ping Parameters window appears (Figure 8-5).

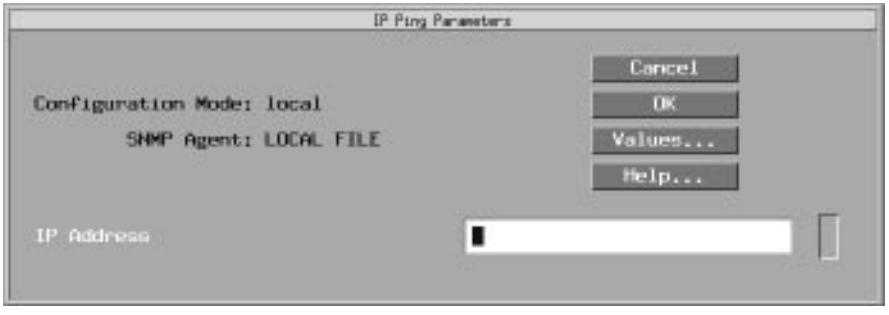

Figure 8-5. IP Ping Parameters Window

7. **Enter the IP address that you want to ping. Then click on OK.**

   You then return to the Ping at Intervals window.

8. **In the display area in the window, click on the IP address for which you want to configure the ping request.**

9. **Enter values for the parameters in the Ping at Intervals window, as described in the next section.**

10. **Click on Apply.**

11. **Click on Ping Start to begin pinging the IP address at the interval you specified.**

    Site Manager stores the results of the ping requests in the Ping MIB tables.

12. **Repeat Steps 8 through 11 to configure (and start) ping requests for additional IP addresses.**

To stop pinging an address, select the address in the Ping at Intervals window and click on Ping Stop.

Specifying Values for Ping at Intervals Parameters

Use the information in this section to specify values for the parameters in the Ping at Intervals window. For each parameter, this section provides information about default settings, valid parameter options, the parameter function, instructions for setting the parameter, and the Management Information Base (MIB) object ID.

The Technician Interface lets you modify parameters by issuing **set** and **commit** commands that specify the MIB object ID. This process is equivalent to modifying parameters using Site Manager.

For more information about using the Technician Interface to access the MIB, refer to *Using Technician Interface Software*.

Caution: *The Technician Interface does not verify that the value you enter for a parameter is valid. Entering an invalid value can corrupt your configuration.*

Parameter:	**IP Address**
Default:	None
Options:	Any valid IP address
Function:	Specifies the IP address of the device you want to ping.
Instructions:	To change the IP address that appears in this field, type the new address in place of the existing one.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.13.1.1.4

Parameter:	**Ping Site Name**
Default:	None
Options:	Any name you want to correspond to the device from which you are pinging
Function:	Serves as descriptive information for your use.
Instructions:	Optionally, enter a name for your ping site.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.13.1.1.17

Parameter:	**Packet Size**
Default:	16
Range:	1 to 4850
Function:	Specifies the size of the Internet Control Message Protocol (ICMP) packet in bytes.
Instructions:	Enter the number of bytes of data that you want to send with each ping.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.13.1.1.5

Parameter:	**Time Out**
Default:	5 seconds
Range:	1 to 65535
Function:	Sets the length of time (in seconds) after which an unsuccessful ping expires.
Instructions:	Enter a value from 1 through 65535.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.13.1.1.6

Parameter:	**Ping Retry**
Default:	1
Range:	1 to 65535
Function:	Specifies the number of successive times to repeat a ping.
Instructions:	Enter a value from 1 through 65535.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.13.1.1.7

Parameter:	**Ping Delay**
Default:	250 milliseconds
Range:	1 to 65535
Function:	Specifies the amount of time (in milliseconds) to wait between sending ICMP echo packets.
Instructions:	Enter a value from 1 through 65535.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.13.1.1.9

Parameter:	**Timer**
Default:	0
Options:	Any integer
Function:	Specifies the number of minutes that will pass before the ping occurs again.
Instructions:	Enter a value (in minutes) or enter 0 if you want to initiate the ping request only once.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.13.1.1.11

Parameter:	**Trace Route**
Default:	PING_NOTRACE
Options:	PING_NOTRACE | PING_TRACE
Function:	Lets you turn on the Trace Routes feature to show the intermediate IP addresses (hops) the ICMP echo packet went through to reach the destination address.
Instructions:	Select PING_TRACE to turn on the Trace Routes feature; otherwise, leave the default, PING_NOTRACE.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.13.1.1.8

Parameter:	**Source Route**
Default:	PING_NOSOURCEROUTE
Options:	PING_NOSOURCEROUTE | PING_STRICTSOURCEROUTE | PING_LOOSESOURCEROUTE
Function:	Lets you override the routing table and specify the alternate addresses you want the ping to go through.
Instructions:	Choose the default PING_NOSOURCEROUTE to use the routing table. Choose PING_STRICTSOURCEROUTE if you want to specify all the IP addresses that the ping *must* go through to reach the destination address. You must know all of the addresses for strict source routing to work. With strict source routing, if the ping cannot get from one of the specified addresses to another, the ping will terminate. Choose PING_LOOSESOURCEROUTE if you want to specify the addresses that the ping *should* go through to reach the destination address; however, the ping might pass through intermediate hops between the addresses you specify. If you choose strict or loose source routing, click on Source Route to specify the routes. See “Specifying Source Routes” later in this chapter.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.13.1.1.12

Parameter:	**Ping Source Address**
Default:	0.0.0.0
Options:	Any valid IP address
Function:	Specifies the IP address of the source of the ping request.
Instructions:	Optionally, enter the IP address you want to use as the source address of the ping request. This should be the IP address of the outgoing port on the router.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.13.1.1.13

Parameter:	**Ping Type of Service**
Default:	NORMAL
Options:	NORMAL | PRIORITY | IMMEDIATE | FLASH | FLASH_OVERRIDE | CRITIC_ECP | INTERNETWORK_CONTROL | NETWORK_CONTROL
Function:	Specifies the quality of service (service precedence) for handling the ICMP packet.
Instructions:	Choose the default NORMAL for routine service, or enter one of the other types of service. Refer to an IP programmer's manual for information on the different types of services.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.13.1.1.14

Parameter:	**Num Hist Buckets Requested**
Default:	1
Range:	1 to 60
Function:	If the ping is on a timer (see the Timer parameter), this parameter specifies the number of entries that you want to store in the Ping History table. In other words, you can save information about each ping request sent on the expiration of a timer. (If the ping is not on a timer, the ping generates only one entry in the history table.)
Instructions:	Enter a number from 1 to 60 to specify the number of instances of the ping you want to save information about in the Ping History table.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.13.1.1.15

Deleting Ping Requests

To remove the results of a ping request from the Ping MIB, follow these steps:

1. **In the display area at the top of the Ping at Intervals window, select the ping request you want to delete.**
2. **Click on Delete.**
3. **Click on Apply or Done.**

   Site Manager removes all entries for the selected request from the appropriate tables.

Specifying Source Routes

If you chose, in the Ping at Intervals window, to use strict or loose source routing (see the description of the Source Route parameter in the previous section), you must specify the routes that you want to use. To do so, click on Source Route in the Ping at Intervals window.

The Source Route Entries window appears (Figure 8-6). Proceed as follows:

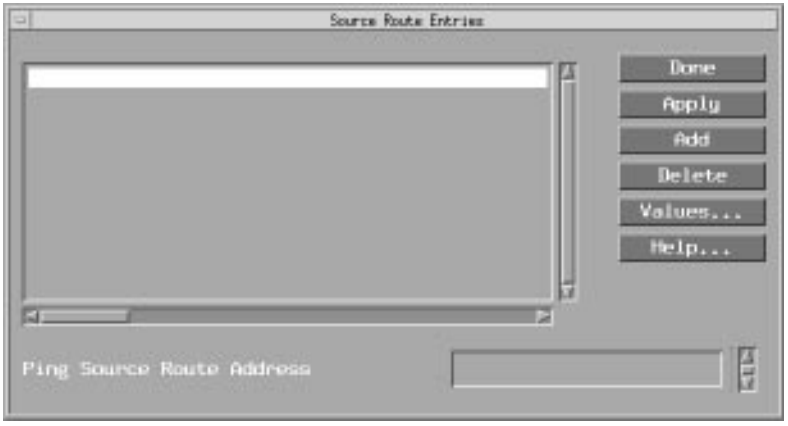

Figure 8-6. Source Route Entries Window

1. **Click on Add.**

   The Source Ping Parameters window appears (Figure 8-7).

Figure 8-7. Source Ping Parameters Window

2. **In the Source Address field, enter the IP address of the device you want the ping to go through to reach its destination. Then click on OK.**

   You return to the Source Route Entries window. The IP address you just entered appears in the display area.

3. **To enter additional source route addresses, repeat Steps 1 and 2.**

   You can enter as many as eight source route addresses. Be sure to enter the source route addresses in the order that you want the packet to traverse them (from source to destination).

4. **Click on Apply, and then click on Done.**

   You then return to the Ping at Intervals window.

Changing or Deleting Source Route Addresses

To change an IP address that appears in the Source Route Entries display window, follow these steps:

1. **Click on the address you want to change.**

   The address appears in the Ping Source Route Address field.

2. **Type the new address in place of the old one.**

3. **Click on Apply (to save your changes and remain in the window), or click on Done (to save your changes and return to the Ping at Intervals window).**

To delete an address from the list of source route addresses, follow these steps:

1. **Click on the address in the display area of the Source Route Entries window.**

2. **Click on Delete.**

3. **Click on Apply (to save your changes and remain in the window), or click on Done (to save your changes and return to the Ping at Intervals window).**

   Site Manager removes the entry from the Source Route Entries window and from the Ping MIB tables.

Reviewing IP Ping Statistics

You can view the information in the Ping MIB using the Statistics Manager in Site Manager. The Statistics Manager provides four default screens that contain information from the Ping MIB. Table 8-1 describes the four screens.

Table 8-1. Default Ping MIB Statistics Screens

Screen Name	Contains Information from
pingmain.dat	Main Ping MIB table
pinghist.dat	Ping history table
pingsrc.dat	Ping source route table
pingtrc.dat	Ping trace route table

Refer to Chapter 4 for information on viewing statistics screens.

Removing Entries from the Ping MIB

You should periodically clear entries from the Ping MIB to prevent the entries from using up too much of your router's memory resources.

To remove entries from the ping tables (main, history, source route, and trace route), follow these steps:

1. **In the Ping at Intervals display window, select the IP address of the device whose ping information you want to remove from the ping tables.**
2. **Click on Delete.**

Appendix A
Responding to SNMP SET Errors

On occasion, you may receive an SNMP SET error. Your Site Manager workstation can display and log all SNMP SET error messages received from a Bay Networks router. Site Manager displays and logs a simple message, `SNMP SET Error` when, for example, you are unable to complete a SET operation because

- An SNMP request from your Site Manager workstation timed out (due to traffic conditions on the network)
- The SNMP community name that you specified for the SNMP request did not allow write-access to the desired router

Figure A-1 shows an example of an SNMP SET error message that appears when a SET *lockout* condition exists on the target router:

```
                SNMP General Set Error!
Machine is currently locked by manager <IP_address>.
```

Figure A-1. Sample SNMP SET Error Message

An SNMP SET error lockout message means that

- The router rejected one or more of your SET attempts.
- You may need to repeat all or part of your configuration task.

For more information on router SNMP SET locking, refer to *Configuring SNMP, BOOTP, DHCP, and RARP Services*.

When you receive an SNMP SET error message, click on OK in the error message box and see if another SET error message pops up immediately. If no other SET error message appears immediately, retry the SET operation.

If several SET error messages appear in succession while you are configuring a circuit in dynamic mode, wait for the router's SNMP lockout condition to clear, and follow these steps:

1. **Delete the circuit you have been attempting to configure.**
2. **Recreate (add) the circuit.**
3. **Repeat all remaining steps of your configuration task.**

If even these steps fail:

1. **Exit from the Configuration Manager without saving your changes.**
2. **Reboot the router on the current (last saved) configuration file.**
3. **Repeat your entire configuration task.**

Accessing the SNMP SET Error Log

As mentioned earlier, your Site Manager workstation can log SNMP SET errors. Figure A-2 shows the logged version of the same SET lockout error message shown in Figure A-1.

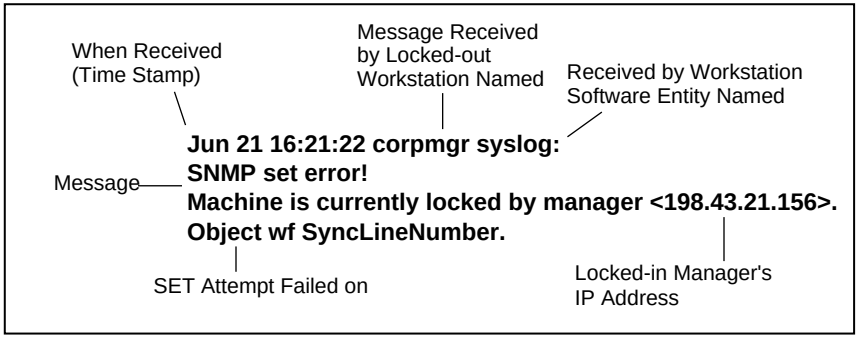

Figure A-2. Logged Version of SNMP SET Error Message

You can examine the default or designated SNMP SET error log file on your Site Manager workstation if you want to analyze an accumulated pattern of SNMP SET errors. The following sections describe how to work with the SNMP SET error log file on UNIX and DOS workstations.

UNIX Workstations

UNIX Site Manager workstations use the standard UNIX *syslog* facility and *syslog.conf* file to specify destinations for SNMP SET error messages. (Refer to the instructions provided in the UNIX man pages for information on *syslog* and *syslog.conf*.)

Examine the <*facility.level*> indicator, `user.err,` in *syslog.conf*. The path specified next to each `user.err` entry indicates a destination for SNMP SET error messages.

Edit *syslog.conf* if you want to respecify destinations for SNMP SET error messages.

DOS Workstations

DOS-based Site Manager workstations log SNMP SET error messages to the *seterror.log* file (*C: \wf \seterror.log*).

Edit *SITEMAN.INI* if you want to

- Switch off SNMP SET error logging (PC platform only).
- Respecify the pathname or filename of the SET error log file.
- Respecify the size of the SET error log file.

Appendix B
Using the *syslog* Facility

Bay Networks provides a *syslog* facility that works with the UNIX *syslogd* daemon residing on remote host systems. The *syslog* facility periodically polls the router's events log and forwards any new router event messages to the remote hosts you specify. The UNIX *syslogd* daemon residing on the remote hosts then outputs the messages to the appropriate device.

If you use Site Manager, you can use the Events Manager to examine router events. However, if you manage your routers using a third-party SNMP-based network management application, such as the Hewlett-Packard OpenView Network Node Manager, then you can use the *syslog* facility as an alternative to SNMP traps to display router events.

You can use the Configuration Manager to configure the *syslog* facility to do the following:

- Deliver event messages in the order in which they occur.
- Filter messages based on a set of criteria that you define.

In addition, you can use the Configuration Manager to enable or disable the *syslog* facility.

You should read this appendix for information on

- Configuring the *syslogd* daemon on remote hosts
- How the *syslog* facility filters event messages
- Configuring the *syslog* facility
- Deleting *syslog* from the router

Configuring the *syslogd* Daemon

You must configure the UNIX *syslogd* daemon to specify the log files and users to which you want to forward event messages. To do this, you must edit the file *etc/syslog.conf* on each remote host. The *syslogd* daemon determines where to write event messages based on

- A *priority code* that the *syslog* application attaches to each event message
- Event data from the *syslog.conf* file

The priority code consists of a *facility* and a *level*. The facility describes the system that originates the event message using the standard (configurable) UNIX facility names LOCAL0 through LOCAL7. The level is the UNIX error level (EMERG, ALERT, CRIT, ERR, WARNING, NOTICE, INFO, DEBUG) that you assign (map) to the severity level (fault, trace, warning, information, and debug) of the router event message.

For example, you might map all router fault messages to the UNIX CRIT error level. You could map more than one router severity level to the same UNIX error level. You can use Site Manager to assign a facility and to map severity levels to error levels, as described later.

For example, suppose you want to log all fault, warning, and debug messages that *syslogd* receives from the router to a file (*/usr/adm/logs/baynet.log*) on the remote host. Assume also that you used Site Manager to map fault messages to the CRIT error level, warning messages to the WARNING error level, and debug messages to the UNIX DEBUG level. You might add a line similar to the following to your *syslog.conf* file:

```
local7.crit;local7.warning;local7.debug /usr/adm/logs/baynet.log
```

In this example, the facility is LOCAL7.

For more information on *syslogd* and *syslog.conf*, refer to the instructions provided in the UNIX man pages.

Understanding How *syslog* Filters Messages

The *syslog* facility forwards router event messages to a remote host only when at least one *entity filter* exists for that host. Entities include Bay Networks software that provides a service, such as TFTP, IP, or the GAME operating system. An entity filter is a set of criteria that you specify to tell *syslog* whether to forward an event message. (Refer to *Event Messages for Routers and BNX Platforms* for a complete list of entities for which you can create filters.)

You can define many entity filters for a remote host, and you can define several different sets of criteria for each entity. For example, you might define two different APPN filters for the same host.

The criteria that define the entity filter can consist of the following:

- The event number or range of numbers. For example, you might want *syslog* to forward only the event messages with event numbers 5 through 50.
- The severity level (warning, fault, trace, informational, or debug).
- The slot or range of slots on which the event occurred. For example, you might want only the event messages that occur on slot 4, or slots 2 through 4.

Note: *The event number and severity level are mutually exclusive.*

Configuring the *syslog* Facility

The steps you must take to configure the *syslog* facility are as follows:

1. **Configure the *syslog* group parameters.**

   The group parameters let you

   — Enable or disable *syslog* on the router.

   — Specify the number of remote hosts you want to configure for *syslog*.

   — Set the polling cycle.

2. **Add at least one remote host for which you want the *syslog* facility to filter and forward router event messages.**

3. **Select a host and add at least one entity filter for that host.**

The following sections describe how to configure and enable the *syslog* facility.

Configuring *syslog* Group Parameters

To configure the *syslog* group parameters, follow these steps:

1. **Bring up the Configuration Manager window.**

   For information on how to do this, refer to *Configuring Routers*.

2. **Select Platform→Syslog→Create Syslog.**

   The Syslog Group Parameters window opens (Figure B-1).

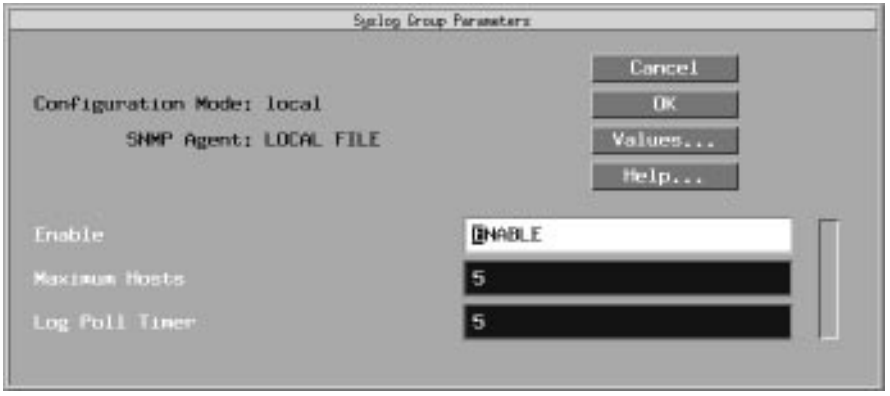

Figure B-1. Syslog Group Parameters Window

3. **Enter values in the Enable, Maximum Hosts, and Log Poll Timer fields, using the following parameter descriptions as a guide.**
4. **Click on OK to exit the window and save your changes.**

Note: *Once you enable* syslog, *you can edit the* syslog *group parameters at any time by selecting Platform→Syslog→Global from the Configuration Manager window.*

syslog Group Parameters

The following is a description of the parameters in the Syslog Group Parameters window (Figure B-1).

For each parameter, this appendix provides information about default settings, valid parameter options, the parameter function, instructions for setting the parameter, and the Management Information Base (MIB) object ID.

The Technician Interface lets you modify parameters by issuing **set** and **commit** commands that specify the MIB object ID. This process is equivalent to modifying parameters using Site Manager. For more information about using the Technician Interface to access the MIB, refer to *Using Technician Interface Software*.

Caution: *The Technician Interface does not verify that the value you enter for a parameter is valid. Entering an invalid value can corrupt your configuration.*

Parameter:	**Enable**
Default:	Enable
Options:	Enable | Disable
Function:	Enables or disables the *syslog* facility on the router.
Instructions:	Set to Disable if you want to disable the *syslog* facility on the router. Note that even though the *syslog* facility is enabled by default, you must use Site Manager to configure a remote host and enable associated filters before the *syslog* facility can filter and forward messages.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.1.2

Parameter:	**Maximum Hosts**
Default:	5
Range:	1 to 10
Function:	Specifies the maximum number of remote hosts you want to configure for the *syslog* facility.
Instructions:	Enter the maximum number of hosts you want to be able to configure for the *syslog* facility.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.1.4

Parameter:	**Log Poll Timer**
Default:	5 seconds
Range:	5 to 610000
Function:	Determines the amount of time (in seconds) *syslog* waits before initiating another cycle to poll all slots for event messages the router logged since the previous polling cycle.
Instructions:	Enter the number of seconds that you want *syslog* to wait between polling cycles.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.1.5

Configuring the *syslog* Host List

You must add the remote hosts for which you want the *syslog* facility to filter and forward router event messages. To do this, follow these steps:

1. **In the Configuration Manager window, select Platform→Syslog→ Syslog Host Table.**

   The Syslog Host List window appears (Figure B-2).

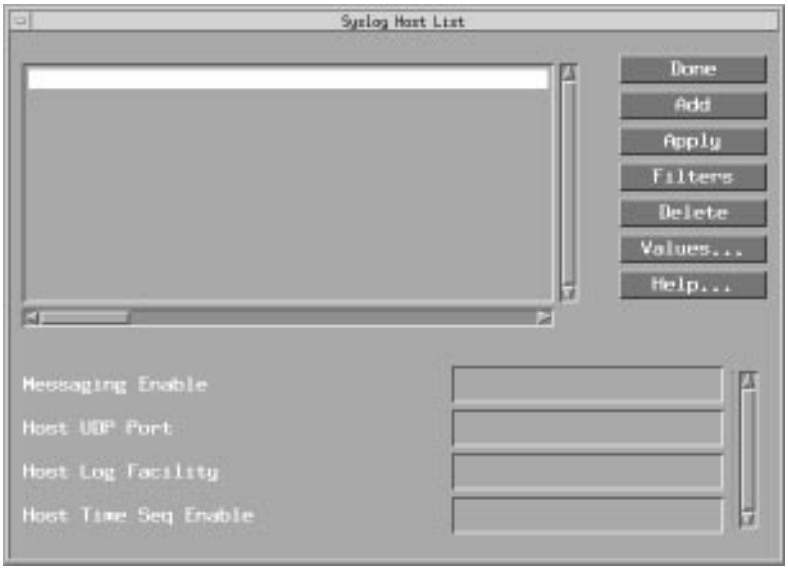

Figure B-2. Syslog Host List Window

2. **Click on Add.**

   The Syslog Remote Host Configuration window appears (Figure B-3).

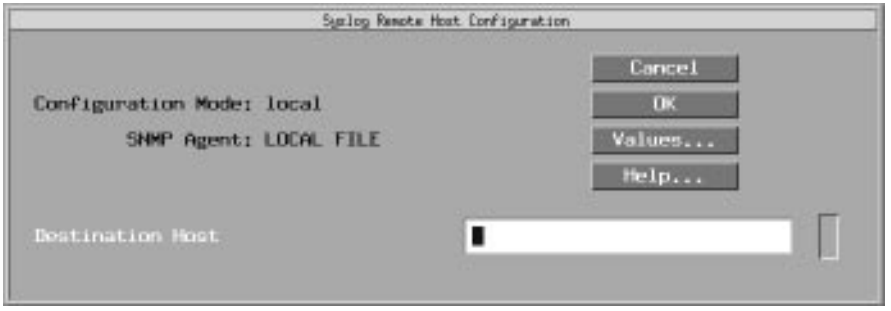

Figure B-3. Syslog Remote Host Configuration Window

3. **In the Destination Host field, type the IP address of the remote host for which you are configuring the *syslog* facility. Then click on OK.**

   The Syslog Host Filter List window appears (Figure B-4).

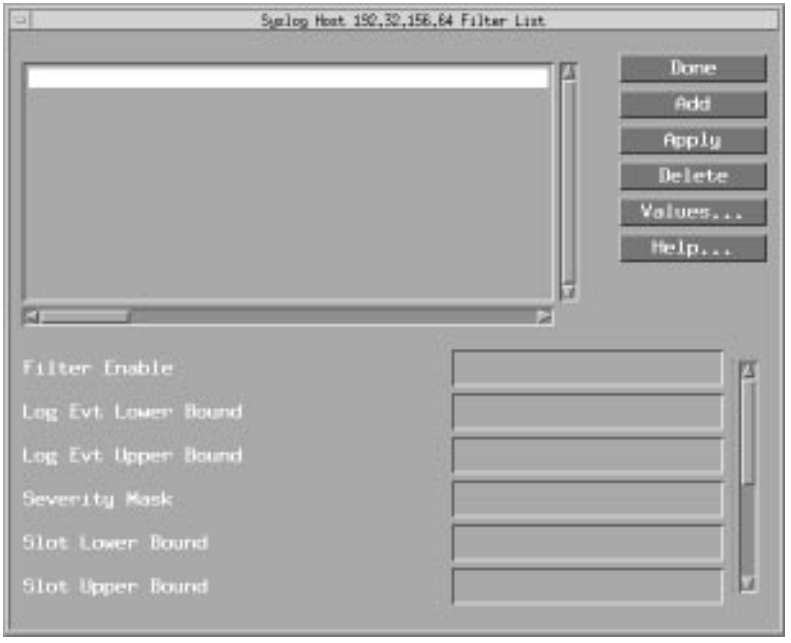

Figure B-4. Syslog Host Filter List Window

4. **Click on Add.**

   The Syslog Filter Config window appears (Figure B-5).

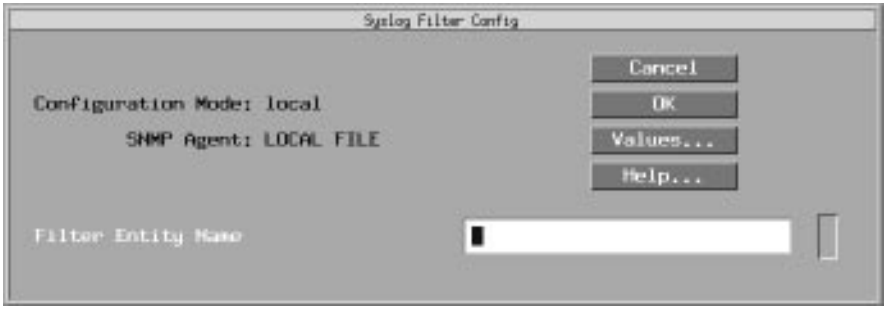

Figure B-5. Syslog Filter Config Window

5. **Enter the Filter Entity Name using the following parameter description as a guide.**

Parameter:	**Filter Entity Name**
Default:	None
Options:	Any valid entity name
Function:	Specifies the entity whose log messages you want to forward to the remote host.
Instructions:	Enter the name of the entity whose log messages you want to forward to the remote host. You can click on Values and select an entity name from the list that appears. Also, *Event Messages for Routers and BNX Platforms* provides a complete list of entity names. If you select the entity name WILDCARD, *syslog* uses the parameters that you specify for this filter only if no other operational filters exist for the remote host. In such cases, *syslog* applies the filters of the wildcard entity to all event messages regardless of the entity.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.3.1.4

6. **Click on OK.**

The Syslog Host Filter List window reappears (Figure B-4). The IP address of the host, the filter number, and filter index appear in the display window.

7. **Define the different aspects of the filter by entering values for the parameters in the Syslog Host Filter List window.**

   Use the descriptions in "Syslog Host Filter List Parameters" as a guide.

8. **Click on Apply.**

9. **To add more filters, click on Add and repeat Steps 5 through 9. Otherwise, click on Done.**

   The Syslog Host List window reappears (Figure B-2).

10. **In the display window, click on the remote host whose parameters you want to configure.**

11. **Enter values for the parameters in the Syslog Host List window. Use the descriptions in the section "Syslog Host List Parameters" as a guide.**

12. **Click on Apply.**

13. **To add more hosts (and filters), repeat Steps 2 through 12. Otherwise, click on Done to save your changes and return to the Configuration Manager window.**

syslog Host Filter List Parameters

The following is a description of the parameters in the Syslog Host Filter List window (refer to Figure B-4).

Parameter:	**Filter Enable**
Default:	Enable
Options:	Enable | Disable
Function:	Enables or disables the filter for the associated remote host.
Instructions:	If you want the *syslog* facility to use this filter to determine which messages to forward to the remote host, select Enable. Otherwise, select Disable. You can stop using this entity filter by deleting the filter. To do this, select the filter in the Syslog Host Filter List window (refer to Figure B-4) and then click on Delete. If you delete an entity filter and later decide you want to use that filter, you must add the filter again.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.3.1.2

Parameter:	**Log Evt Lower Bound**
Default:	0
Range:	0 to 255
Function:	Along with the Log Evt Upper Bound parameter, this parameter specifies the event number (code) or range of event numbers (for the current filter) that you want to forward to the remote host. Refer to *Event Messages for Routers and BNX Platforms* for a complete list of event codes for each entity.
Instructions:	To specify a range of event numbers that you want to use in the filter, enter the lower number of the range in this field. You then enter the upper number of the range in the Log Evt Upper Bound field described next. The values you enter for lower and upper bound are included in the range. For example, if you specify a lower bound of 2 and an upper bound of 7, *syslog* forwards all messages that are of event codes 2 through 7 (inclusive). The *syslog* facility ignores all other event messages. To filter a specific event code, enter the event code in this field. Be sure to enter the same code in the Log Evt Upper Bound field. For example, to forward only the log messages that have an event code of 10, enter 10 in this field and in the Log Evt Upper Bound field. If you do not want to filter by event code, accept the default, 0. Be sure to do the same in the Log Evt Upper Bound field. If you use a wildcard filter entry, the *syslog* facility ignores this parameter.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.3.1.7

Parameter:	**Log Evt Upper Bound**
Default:	255
Range:	0 to 255
Function:	Along with the Log Evt Lower Bound parameter, this parameter specifies the event number (code) or range of event numbers (for the current filter) that you want to forward to the remote host. Refer to *Event Messages for Routers and BNX Platforms* for a complete list of event codes for each entity.
Instructions:	To specify a range of event numbers, enter the upper number of the range in this field. You must specify the lower number of the range in the Log Evt Lower Bound field described previously. To filter a specific event code, enter the event code in this field. You must enter the same event code in the Log Evt Lower Bound field. If you do not want to filter by event code, accept the default, 255. Be sure to do the same in the Log Evt Lower Bound field. If you use a wildcard filter entry, the *syslog* facility ignores this parameter.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.3.1.8

Parameter:	**Severity Mask**
Default:	None
Options:	w (warning) | i (informational) | t (trace) | f (fault) | d (debug)
Function:	Identifies the types of events (warning, informational, trace, fault, debug) to forward only if the range of event numbers includes all events (0 through 255). The *syslog* facility ignores any events that are not of the types you specify.
Instructions:	If you specified a range of event numbers (using the Log Evt Lower Bound and Log Evt Upper Bound parameters), *syslog* ignores the Severity Mask parameter. If you did not specify a range of event numbers, enter the types of events you want to forward. Use the first letter of each event type you want to include: w – warning i – informational t – trace f – fault d– debug Be sure to enter lowercase letters only. Do not separate the letters with commas or spaces.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.3.1.9

Parameter:	**Slot Lower Bound**
Default:	0
Range:	0 to 14
Function:	Along with the Slot Upper Bound parameter, this parameter specifies the slot or range of slots on which you want to filter the log messages for this entity. (In the case of ASN routers, this parameter specifies the module for the particular slot since an ASN router is considered a slot.)
Instructions:	To specify a range of slots, enter the lower number of the range in this field. You then enter the upper number of the range in the Slot Upper Bound field described next. The values you enter for lower and upper bound are included in the range. For example, if you specify a lower bound of 1 and an upper bound of 4, *syslog* forwards all messages that occur on Slots 1 through 4 (inclusive). The *syslog* facility ignores event messages that occur on all other slots. To filter events for a specific slot, enter the slot number in this field. Be sure to enter the same number in the Slot Upper Bound field. For example, to forward only the log messages that occur on Slot 2, enter 2 in this field and in the Slot Upper Bound field. If you do not want to use this filter, accept the default, 0. Be sure to do the same in the Slot Upper Bound field.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.3.1.10

Parameter:	**Slot Upper Bound**
Default:	0
Range:	0 to 14
Function:	Along with the Slot Lower Bound parameter, this parameter specifies the slot or range of slots on which you want to filter the log messages for this entity.
Instructions:	To specify a range of slots, enter the upper number of the range in this field. You must specify the lower number of the range in the Slot Lower Bound field, as described previously. To filter events for a specific slot, enter the slot number in this field. You must enter the same number in the Slot Lower Bound field. If you do not want to use this filter, accept the default, 0. Be sure to do the same in the Slot Lower Bound field.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.3.1.11

Parameter:	**Fault Map**
Default:	CRIT
Options:	EMERG | ALERT | CRIT | ERR | WARNING | NOTICE | INFO | DEBUG
Function:	Maps router event messages with a severity level of fault to an error level that UNIX *syslogd* recognizes. Table B-1 describes each of these error levels.
Instructions:	We recommend you accept the default UNIX error level for this severity level. To map this severity level to a different UNIX error level, click on Values, and then select the error level you want.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.3.1.12

Table B-1. *syslogd* Error Levels

Error Level	Description
EMERG	A panic condition that *syslogd* normally broadcasts to all users
ALERT	A condition, such as a corrupted system database, that you should correct immediately
CRIT	Critical conditions, such as hard device errors
ERR	Errors
WARNING	Warning messages
NOTICE	Conditions that are not errors, but that may require special handling
INFO	Informational messages
DEBUG	Messages that contain information that is of value only when you are debugging the network

Parameter: **Warning Map**

Default: WARNING

Options: EMERG | ALERT | CRIT | ERR | WARNING | NOTICE | INFO | DEBUG

Function: Maps router event messages with a severity level of warning to an error level that UNIX *syslogd* recognizes. See Table B-1 for a description of the *syslogd* error levels.

Instructions: We recommend you accept the default UNIX error level for this severity level. To map this severity level to a different UNIX error level, click on Values, and then select the error level you want.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.15.3.1.13

Parameter:	**Info Map**
Default:	INFO
Options:	EMERG | ALERT | CRIT | ERR | WARNING | NOTICE | INFO | DEBUG
Function:	Maps router event messages with a severity level of info to an error level that UNIX *syslogd* recognizes. See Table B-1 for a description of the *syslogd* error levels.
Instructions:	We recommend you accept the default UNIX error level for this severity level. To map this severity level to a different UNIX error level, click on Values, and then select the error level you want.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.3.1.14

Parameter:	**Trace Map**
Default:	DEBUG
Options:	EMERG | ALERT | CRIT | ERR | WARNING | NOTICE | INFO | DEBUG
Function:	Maps router event messages with a severity level of trace to an error level that UNIX *syslogd* recognizes. See Table B-1 for a description of the *syslogd* error levels.
Instructions:	We recommend you accept the default UNIX error level for this severity level. To map this severity level to a different UNIX error level, click on Values, and then select the error level you want.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.3.1.15

Parameter:	**Debug Map**
Default:	DEBUG
Options:	EMERG | ALERT | CRIT | ERR | WARNING | NOTICE | INFO | DEBUG
Function:	Maps router event messages with a severity level of debug to an error level that UNIX *syslogd* recognizes. See Table B-1 for a description of the *syslogd* error levels.
Instructions:	We recommend you accept the default UNIX error level for this severity level. To map this severity level to a different UNIX error level, click on Values, and then select the error level you want.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.3.1.16

syslog Host List Parameters

The following is a description of the parameters in the Syslog Host List window (Figure B-2).

Parameter:	**Messaging Enable**
Default:	Enable
Options:	Enable | Disable
Function:	Enables or disables the forwarding of router events to this remote host.
Instructions:	If you want *syslog* to forward router events to this host, accept the default. If you do not want *syslog* to forward events to this host, select Disable. You can also stop forwarding router events to the host by deleting the host. To do this, select the remote host in the Syslog Host List window (Figure B-2) and then click on Delete. If you delete a remote host and later decide you want to forward router events to that host, you must add the remote host again.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.2.1.2

Parameter:	**Host UDP Port**
Default:	514
Range:	514 to 530
Function:	Identifies the UDP port of the remote host.
Instructions:	Type the port number to which you want *syslog* to send UDP packets.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.2.1.4

Parameter:	**Host Log Facility**
Default:	LOCAL7
Options:	LOCAL0 to LOCAL7
Function:	Specifies the facility type that *syslog* appends to router event messages as part of the priority code. (See "Configuring the *syslogd* Daemon" earlier in this chapter for more information on the priority code.) The *syslogd* daemon on the remote host uses this information to determine which system generated the message that *syslog* forwarded.
Instructions:	Enter the facility type you want to use. You must also specify the facility type in the *syslog.conf* file on the remote host as part of your entry that tells *syslogd* where to direct event messages from this facility.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.2.1.5

Parameter:	**Host Time Seq Enable**
Default:	Disable
Options:	Enable | Disable
Function:	Forwards (to the remote host) router event messages in the order that they occur.
Instructions:	Enable this feature only if it is essential that the remote host receive router event messages in the order that they occur. When this feature is enabled, the *syslog* facility polls the router events log, filters the messages, orders them based on the time they occurred, and then forwards them to the remote hosts. When this feature is disabled, the *syslog* facility polls the router events log, filters the messages, and then forwards the messages to the remote hosts.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.2.1.6

Deleting the *syslog* Facility from the Router

To delete the *syslog* facility from the router, follow these steps:

1. **In the Configuration Manager window, select Platform→Syslog→Delete Syslog.**

   A window prompts you to confirm your decision:

   ```
   Do you REALLY want to delete Router Syslog?
   ```

2. **Click on OK in the confirmation window.**

Appendix C
Generating Binary Configuration Files

Config Generator (rpt2cfg) is a UNIX command-line tool that you use to create bootable binary configuration files from your edited ASCII configuration file reports. With Config Generator, you can create configuration files faster than with the Site Manager Configuration Manager.

Caution: *Config Generator is meant for advanced users only. It provides very limited validation checking of the edited ASCII configuration file. If you attempt to boot from a corrupt configuration file the results will be unpredictable. The router or platform may fail diagnostics or fail to boot.*

Make sure you are familiar with the ASCII configuration file format and know exactly what changes to make before you use Config Generator. For additional information or advice, contact the Bay Networks Technical Response Center.

To create a bootable binary configuration file with Config Generator you need to

- Use Report Generator to create an ASCII configuration file report (see Chapter 6).
- Use a text editor to make changes to the file.
- Use Config Generator to convert the edited ASCII configuration file report to a bootable binary configuration file.

Preparing the ASCII Configuration File

Config Generator requires that you include the Bay Networks MIB names in the ASCII configuration file report. Choose the appropriate option when you generate your report:

- If you are using Report Generator from Site Manager, select the **Show MIB Names** option from the Output Format Options dialog box.

- If you are using Report Generator from the UNIX or Windows command line, use the **-m** option.

You can select any of the other options you want to include in the ASCII configuration file report, as long as you include the MIB names. Refer to Chapter 6 for more information on generating an ASCII configuration file report.

Caution: *You must include the MIB Names in the ASCII configuration file for Config Generator to create a valid binary configuration file.*

Using Config Generator

Config Generator is available to users of Site Manager Version 4.0 (or BNX Version 6.0) or later. Config Generator is located in the */usr/wf/bin* directory along with the other Site Manager command line tools.

You run Config Generator from the UNIX command line. Enter the name of the edited ASCII configuration file you want to convert, and a name for the new binary configuration file, in the following format:

rpt2cfg -f*<ASCII Report Filename>* [**-o***<New Binary Filename>*]

If you don't supply a new binary filename, Config Generator sends the output to *<stdout>*.

Depending on the size of the file, Config Generator may take several minutes to convert the file. When Config Generator is finished, the UNIX prompt returns. If no error messages appear, Config Generator created and saved the binary configuration file. If you receive an error message, the file is corrupt and should not be used.

Checking for Errors

Config Generator checks the ASCII configuration file for valid MIB names, valid MIB values, and for duplicate circuit names. If these errors are found, Config Generator displays the line number in the ASCII configuration file where the error occurred, and a brief description of the error. The program does not check for cross-dependencies within the file.

Correct any errors in the ASCII configuration file report and run Config Generator on the corrected file. When you are satisfied that you have a valid binary configuration file, use TFTP to transfer the file to the router or platform and reboot (see Chapter 5 for more information on TFTP). Remember that Config Generator provides very limited error checking. Always keep a valid binary configuration file ready in case the boot fails.

Checking MIB Attributes

You can use Config Generator to find the possible MIB attributes for a particular MIB record. To find the possible attributes, you provide the MIB name and MIB version number in the following format:

rpt2cfg -q *<MIB Name>* **-d***<MIB Version Number>*

where *MIB Version Number* is equal to the current software version number (7.80, 8.00, 8.10, 10.0, etc.). For example, to find the MIB attributes for the 8.10 version of the MIB record `wfsys` enter the following:

```
rpt2cfg -q wfsys -d 8.10
```

Config Generator displays

```
Possible valid attributes for this record entry are:
wfSysContact
wfSysName
wfSysLocation
wfSysMibRevision
wfSysMibCounterEnable
```

Checking MIB Attribute Values

You can use Config Generator to find a range of valid values for a given MIB attribute. To find the values, you provide the MIB attribute and the MIB version number in the following format:

rpt2cfg -q *<MIB Attribute>* **-d***<MIB Version Number>*

where *MIB Version Number* is equal to the current software version number (7.80, 8.00, 8.10, 10.0, etc.). For example, to find the values for the 8.10 version of the MIB attribute `wfSysMibCounterEnable` enter the following:

```
rpt2cfg -q wfSysMibCounterEnable -d 8.10
```

Config Generator Displays

```
Possible valid list of values are:
DISABLE, ENABLE
```

Identifying Files Created by Config Generator

Config Generator adds a text string to the system name of the configuration files it generates so that you can differentiate them from other configuration files. To see the message, start at the Site Manager Configuration Manager window and select Platform→Edit System Information. The following message is added to the System Name field:

```
/This binary config was created using rpt2cfg
```

You will also see this message in any ASCII configuration file reports that you create with Report Generator from binary configuration files that you created with Config Generator. You can see the message on the line in the file that identifies the system name.

Index

A

access information about MIB objects, 4-8
ace.out, 5-5, 7-4
ACE32, 7-31, 7-32, 7-35
address
  filters, 2-19
    default setting, 2-19
  MAC, 4-29
  mask, 4-23
Administration menu, 1-15, 7-1
AFN, 5-5, 7-31, 7-35
afn.exe, 5-5
agent
  SNMP
    configuring, 2-2 to 2-6
    enabling, 2-14
aliases in debug.al file, 5-6
ALL trap category, 2-10
ALN, 5-5, 7-31
AN, 5-5, 7-31, 7-35
  partitioning media on, 5-3, 5-26 to 5-30
an.exe, 5-5
APING, 7-29
AppleTalk Ping, 7-27
APPN Ping, 7-29 to 7-31
ARP, 7-20
ASCII file
  converting to binary, C-1
  saving event messages to an, 1-8, 3-9
  saving statistics to an, 4-27
  saving trap messages to an, 2-21
ASN, 5-5, 7-31, 7-35
  partitioning media on, 5-3, 5-26 to 5-30
asn.exe, 5-5
asndiag.exe, 5-5
audit trail logging, 6-11 to 6-13
automatic overwrite, 5-8, 5-19
available free space, 5-4, 5-25

B

backing up router files, 5-5, 5-23, 5-25
backplane ID, 4-6
Bay Networks
  MIB, 1-9, 4-3, 4-5
  software, B-3
BCN, 7-31
binary format
  converting to, C-1
  default configuration file, 5-5
  event logs in, 1-8, 3-2, 3-10
  ti.cfg file, 5-6
BLN, 7-31
BLN-2, 7-31
BN, 5-5
bn.exe, 5-5
BNX, 5-5
boot
  command, 5-5
  delayed, 7-4
  FN/LN/CN, 7-2
  image, 5-5, 5-6, 7-3, 7-35

processor module, 7-13
PROM, 5-6
router, 7-1, 7-3
slot, 7-13
verification, 7-4

C

categories of traps, 2-9
circuit
mode
statistics screens, 1-11, 4-17, 4-32
name table, 4-6
clearing
counter objects, 4-18
event log, 3-11, 7-15
Events Manager window, 3-9
trap history file, 2-20
CLNP echo request, 7-22
CN, 5-5, 7-31
code
entity, 1-5, 2-13
event, 1-5, 2-13
cold-starting a router, 7-1
column, setting up in statistics screens, 4-29
communities, SNMP, 2-4
compacting memory, 5-24
config file, 7-4
converting from ASCII to binary, C-1
Config Generator, using, C-2
configuration
file, 5-5, 5-8
audit trail, 6-11
converting from ASCII to binary, C-1
generating report of, 6-1 to 6-10
logging changes to, 6-11 to 6-13
remote, 5-23
saving, 2-5
Configuration Manager
setting up SNMP on a router, 2-2
tool, 1-3
configuring
IP Ping requests for Ping MIB, 8-1 to 8-11
kernel, 7-31, 7-34
traps
by category, 2-8
by entity, 2-10
by event type, 2-12
connection to router, 2-1, 3-1, 4-2
console in wfSystem MIB object group, 4-6
contiguous free space, 5-4, 5-25
Control Point name, 7-29
conventions for filenames, 5-7
copying router files, 5-8
counters, zeroing, 4-18
counters, MIB II, 4-35
current screen list, 1-11, 4-13, 4-15
custom screen directories, 1-12, 4-33
customizing statistics screens, 1-11, 4-28 to 4-33

D

date for router, 7-15
Debug Map parameter, B-19
debug messages, 2-10
debug.al, 5-6
debugging network, 1-10, 5-6
decimal format, displaying statistics in, 4-29
Dedicated to Global Pool field, 7-35
default
address filter, 2-19
button, 7-35
configuration file, 5-5, 5-8
router software image, 7-2
slot, 7-13
statistics screens, 4-13, 4-14, 4-33
Delayed Boot
deleting, 7-9
enabling and disabling, 7-5
modifying, 7-9

parameters, 7-10
scheduling, 7-5
using, 7-4
deleting
Delayed Boot, 7-9
IP Ping requests from Ping MIB, 8-11
media partition, 5-30
router files, 5-10
Destination Host parameter, B-8
diagnosing network problems, 3-7
diagnostics
command, 7-1
image, 5-6
PROM, 5-6
tests, 7-1
diskette, router software on, 5-3
display
Site Manager, refreshing, 7-4
statistics, refreshing, 4-23
Display Filters window, 4-22
displaying
statistics, 4-16
custom screens, 4-33
volume contents, 5-2
dynamic mode, performing, 1-2

E

editing
audit trail configuration file, 6-11
SNMP global parameters, 2-14
statistics files, 4-34
Enable parameter (syslog), B-5
enabling SNMP agent, 2-14
entity
code, 1-5, 2-13
specifying an, 2-10
erasing memory cards, 5-24
event
code, 1-5, 2-13
log, 1-3, 7-35
clearing, 3-11
current, 3-2
displaying, 3-2
local, 3-5
remote, 3-4
message
looking up, 1-8
record, 3-7
saving, 3-9
searching for, 3-8
Events Manager
tool, 1-8, 3-1
window, 1-7, 3-4
clearing, 3-9
refreshing, 3-9
exiting Site Manager, 2-7

F

Fault Map parameter, B-16
fault messages, 2-10
FDDI tables, 4-6
file
backup, 5-23, 5-25
compacting, 5-25
configuration, 5-5, 5-8
audit trail, 6-11
generating report of, 6-1 to 6-10
copying, 5-8
deleting, 5-10
extensions, 4-14, 5-7
naming conventions, 5-7
partition, 5-29
remote configuration modifications, 5-23
retrieving, 5-16
statistics, 1-12
retrieving, 4-33
syslog.conf, B-2
transfer, 5-11
trap history, 1-3, 2-16
clearing, 2-20

filter
address, 2-19
by display string, 4-22
creating, 4-21
Quick Get retrieval, 4-8
statistics display, 4-21
statistics retrieval, 4-21, 4-25
traps, 2-17 to 2-20
by IP address, 2-18
by severity, 2-18
Filter Enable parameter, B-11
Filter Entity Name parameter, B-9
Filtering Parameters window, 3-7
Find Text Pattern window, 3-8
FN, 5-5, 7-31
formatting memory cards, 5-26
FRE2, 7-31, 7-32, 7-35
freboot.exe, 5-6
frediag.exe, 5-6
free space, 5-4

G

GAME, B-3
generating configuration file report, 6-1 to 6-10
format options, 6-2
from UNIX, 6-8
from Windows, 6-9
specifying a template, 6-6
GENERIC trap category, 2-9
Get Remote Log File window, 3-4
getting files, 5-16
global memory, 7-35
Greenwich mean time, 7-16

H

hexadecimal format
displaying statistics in, 4-29
network and host addresses, 7-25, 7-27
host
address, 7-25
ID, 7-25
mode, running IP in, 5-13, 5-19
host list for syslog, B-7 to B-21
Host Log Facility parameter, B-20
Host Time Seq Enable parameter, B-21
Host UDP Port parameter, B-20

I

ICMP echo request, 7-17
ID
network, 7-25
Site Manager workstation, 2-3
ifInNUcastPkts counter, 4-35
ifInUcastPkts counter, 4-35
ifInUnknownProtos counter, 4-35
ifOutNUcastPkts counter, 4-35
ifOutUcastPkts counter, 4-35
image
boot, 5-5, 5-6, 7-3, 7-35
diagnostics, 5-6
router default, 7-2
Info Map parameter, B-18
information messages, 2-10, 2-18
interface drivers, 4-6
IP
address filters, 2-18
routes, 7-35
routing statistics, 4-14
IP address parameter, 8-7
IP Ping, 7-17 to 7-20
configuring requests for Ping MIB, 8-1 to 8-11
deleting requests from Ping MIB, 8-11
specifying source routes, 8-12 to 8-13
statistics, 8-14
IPX Ping, 7-20 to 7-22

K

kernel configuration, 7-31, 7-34

L

Launch Facility tool, 4-16
line state and traffic, 4-6
LN, 5-5, 7-31
Load Local Log File window, 3-5
Load Screen window, 4-32
local memory, 7-35
locked message, A-1
log
  audit trail, 6-11 to 6-13
  events, 1-3
    clearing, 3-11
    current, 3-2
    displaying, 3-2
    local, 3-5
    remote, 3-4
    searching for, 3-8
Log Evt Lower Bound parameter, B-12
Log Evt Upper Bound parameter, B-13
Log Poll Timer parameter, B-6
loose source routing, 8-10

M

MAC address, 4-29, 7-19
manager
  adding, 2-5
  SNMP, 2-4
Maximum Hosts parameter, B-6
media partitioning, 5-3, 5-26 to 5-30
memory
  card
    compacting, 5-24
    erasing, 5-24
    formatting, 5-26
    router software on, 5-3
  global, 7-35
  local, 7-35
  module, router software on, 5-3
  partitioning, 7-31
Messaging Enable parameter, B-19
MIB
  Bay Networks, 1-9, 4-3, 4-5
  browser, 4-3, 4-5, 4-6, 4-7, 4-29
  description, 1-10
  object groups, 4-6
  Objects window, 4-4
  Ping, 1-16, 8-1
    configuring IP Ping requests, 8-1 to 8-11
    deleting IP Ping requests, 8-11
    specifying IP Ping source routes, 8-12 to 8-13
    viewing IP Ping statistics, 8-14
  standards, 4-37
  variables, 5-6
  viewing, 1-9
MIB II Counters feature, 4-35
modifying configuration files, 5-23
monitoring traps, 2-16
multiple routers, setting up, 5-13

N

naming files, 5-7
network ID, 7-25
network management applications, 2-6
NONE trap category, 2-9
NSAP address, 7-23, 7-24
Num Hist Buckets Requested parameter, 8-11
NVRAM, 7-32, 7-35

O

object
  groups, 4-5, 4-6
  MIB, 4-4

type, 4-8
OSI Ping, 7-22 to 7-24
overwrite, 5-8, 5-19

P

packet information, 4-6
Packet Size parameter, 8-7
parameters
editing SNMP global, 2-14
enabling SNMP agent, 2-14
partitioning media, 5-26 to 5-30
partitioning memory, 7-31
Ping
AppleTalk, 7-27
APPN, 7-29 to 7-31
IP, 7-17 to 7-20
IPX, 7-20 to 7-22
MIB, 1-16, 8-1
configuring IP Ping requests, 8-1 to 8-11
deleting IP Ping requests, 8-11
specifying IP Ping source routes, 8-12 to 8-13
viewing IP Ping statistics, 8-14
OSI, 7-22 to 7-24
remote devices, 7-16
router, 5-19
VINES, 7-24 to 7-26
Ping Delay parameter, 8-8
Ping Retry parameter, 8-8
Ping Site Name parameter, 8-7
Ping Source Address parameter, 8-10
Ping Type of Service parameter, 8-11
polling
rate, 1-11, 4-17
router, 1-9, 4-17
power supply, router, 4-6
previewing statistics screens, 4-31
processor module
booting, 7-13
partitioning memory, 7-31
PROM, 5-6
boot, 5-6
diagnostic, 5-6
protocol state information, 4-6
putting files on multiple routers, 5-13

Q

Quick Get
Facility window, 4-3, 4-8
retrieval filter, 4-8
tool, 1-10, 4-3

R

Radix field, 4-29
reallocating memory, 7-31
real-time display of trap messages, 2-16
refreshing
Events Manager window, 3-9
Site Manager window, 7-4
statistics, 4-17, 4-23
remote configuration mode, 5-23
description of, 1-2
report
generating from configuration file, 6-1 to 6-10
format options, 6-2
from UNIX, 6-8
from Windows, 6-9
specifying a template, 6-6
Reset button, 7-1
resetting a slot, 7-13
retrieval filter
Quick Get, 4-8
statistics, 4-21, 4-25
window, 4-25
Retrieve Request option, 4-13
router
backplane ID, 4-6

boot procedures, 7-1
circuit name table, 4-6
cold-starting, 7-1
connection, 2-1, 3-1, 4-2
date and time, 7-15
default software image, 7-2
Ping, 5-19, 7-16
polling, 4-17
power supply, 4-6
serial number, 4-6
system record, 4-6
temperature, 4-6
warm-starting, 7-1
Router Date and Time window, 7-15
routes, IP, 7-35
routing tables, 4-6, 7-15
rptrAddrTrackPackage, 4-5, 4-6
rptrBasicPackage, 4-5, 4-6
rptrMonitorPackage, 4-5, 4-6
RUI Boot, 7-4

S

Save Log window, 3-10
saving
configuration, 2-5
event messages, 3-9
trap messages, 2-21
Screen Builder Facility window, 4-28
Screen Builder tool, 1-11, 4-33, 4-34
Screen Launch Facility tool, 1-11, 4-16
Screen Manager tool, 1-11, 4-13
screens
default statistics, 4-14
designing for statistics, 4-28
Search Options window, 4-26
searching the event log, 3-8
Selected Trap Types window, 2-18
serial number for router, 4-6
Set Address Filters option, 2-17
SET error, A-1
severity
filtering events by, 3-6
messages, 2-18
Severity Mask parameter, B-14
Site Manager
Administration menu, 1-15
exiting, 2-7
restarting from command line, 2-7
workstation ID, 2-3
slot
default, 7-13
filtering events by, 3-6
reset, 7-13
Slot Lower Bound parameter, B-15
Slot Upper Bound parameter, B-16
SNMP, A-1
acronym, 1-2
adding a Manager, 2-5
agent, 1-3, 1-5
configuring, 2-2 to 2-6
enabling, 2-14
specifying an entity, 2-10
Community List window, 2-4
editing global parameters, 2-14
Manager List window, 2-4
polling, 1-9
trap port, 2-6
Source Route parameter, 8-9, 8-10
source routes, specifying for IP Ping, 8-12
SPECIFIC trap category, 2-10
statistics
customizing screens for, 1-11, 4-28
database of screens for, 1-11
default screens for, 4-13, 4-14, 4-33
description of, 1-9
display filter for, 4-21
displaying, 4-16
files, 1-12, 4-32
editing, 4-34

retrieving, 4-33
filter for, 4-21
generating totals of, 4-30
IP Ping, 8-14
IP routing, 4-14
refreshing screen, 4-17
retrieval filters for, 4-21, 4-25
updating, 4-17
Statistics Manager
tool, 1-9, 4-15
Tools menu, 1-9
window, 4-2
strict source routing, 8-10
syntax for MIB objects, 4-8
SYSCON, 7-32
syslog, 1-2
adding remote hosts for, B-7
configuring group parameters for, B-4 to B-6
configuring the host list for, B-7 to B-21
deleting from the router, B-21
filtering event messages with, B-3
syslog.conf file, B-2
syslogd daemon, configuring, B-1
system record for router, 4-6

T

table mode screens, 1-12, 4-32
Technician Interface, 5-6
diags command, 7-1
temperature of router, 4-6
templates for configuration file reports, 6-3
test
diagnostics, 7-1
Ping, 5-19, 7-16
TFTP, 5-12
ti.cfg, 5-6
Time Out parameter, 8-8
time, setting on router, 7-15
Timer parameter, 8-9
Toggle button, Filtering Parameters, 3-6
tools
Events Manager, 1-8, 3-1
Launch Facility, 1-11, 4-16
Screen Builder, 1-11, 4-33, 4-34
Screen Manager, 1-11, 4-13
Statistics Manager, 1-9, 4-15
Trap Monitor, 2-1
totals, generating from statistics, 4-30
Trace Map parameter, B-18
trace messages, 2-10
Trace Route parameter, 8-9
transferring files, 5-11, 5-19
trap history file, 1-3, 2-16
clearing, 2-20
Trap Monitor tool, 1-3, 2-1, 2-17
traps
adding, 2-13
categories of, 2-9
clearing from Trap Monitor window, 2-20
configuring
by category, 2-8
by entity, 2-10
by event type, 2-12
exceptions lists, 2-12, 2-14
filtering, 2-17 to 2-20
by IP address, 2-18
by severity, 2-18
monitoring, 2-16
port, 2-6, 2-7
saving, 2-21
types, 2-7, 2-17, 2-18
viewing, 1-4, 2-16
troubleshooting, 7-13
type, MIB object, 4-8

U

UDP, port for traps, 2-6
UNIX syslogd daemon, B-1
configuring, B-2

V

viewing
event messages, 3-2
trap messages, 2-16
VINES Ping, 7-24 to 7-26
VME, 7-31
volume
displaying contents, 5-2
number, 7-4
partitioning, 5-3, 5-26 to 5-30

W

warm-starting router, 7-1
Warning Map parameter, B-17
warning messages, 2-10, 2-18
wfApplication, 4-5, 4-6, 4-7
wfHardwareConfig, 4-5, 4-6
wfLine, 4-5, 4-6
wfSoftwareConfig, 4-5, 4-6
wfSystem, 4-5, 4-6
workstation ID, 2-3

Z

zeroing counter objects, 4-18